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

BACHELOR UNIVERSITAIRE DE TECHNOLOGIE

**RÉSEAUX ET TÉLÉCOMMUNICATIONS, PARCOURS CYBERSÉCURITÉ**

# ÉVALUATION DE COMPÉTENCE C8 : SENSIBILISER AUX VULNÉRABILITÉS D'UN SYSTÈME D'INFORMATION ET AUX REMÉDIATIONS POSSIBLES

SESSION 2026

Durée : 2 heures

| SPÉCIALITÉ / UNITÉ | COEFF |
|---|---|
| RÉSEAUX ET TÉLÉCOMMUNICATIONS, PARCOURS CYBERSÉCURITÉ | 3 (INDICATIF) |

Moyens de calculs et matériel autorisés :

**L'usage de la calculatrice n'est pas autorisé.**

**Aucun document ou matériel autorisé en dehors de ceux fournis avec le sujet.**

Dès que le sujet vous est remis, assurez-vous qu'il est complet.

Ce sujet comporte 9 pages numérotées de 1/9 à 9/9.

Les documents réponses en fin de sujet sont à rendre avec la copie.

# DOSSIER SUJET

## MISE EN SITUATION PROFESSIONNELLE ET CONSIGNES GÉNÉRALES : ALPINA SERVICES NUMÉRIQUES, PME DE SERVICES INFORMATIQUES, ANNECY (HAUTE-SAVOIE)

Vous intervenez comme technicienne ou technicien au sein de l'équipe informatique d'Alpina Services Numériques. La direction vous demande d'examiner une architecture simplifiée, de signaler les vulnérabilités compréhensibles par les responsables de l'entreprise et de proposer des actions de remédiation adaptées.

L'entreprise compte 68 salariés. Son système d'information héberge une application de gestion commerciale, un espace de fichiers partagé et une application RH contenant des données personnelles. Les éléments utiles à l'analyse figurent dans les documents DT 1 à DT 3. Les échelles de vraisemblance et d'impact ainsi que les seuils de criticité sont définis dans le DT 2 et doivent être utilisés pour toutes les évaluations demandées.

Répondez dans les documents réponse DR 1 et DR 2. Toute proposition doit être justifiée par un élément du dossier. Le barème est de 20 points.

## PARTIE 1 : Comprendre le système d'information et qualifier les enjeux (4 points)

***Identification des actifs, des données et des enjeux de sécurité***

À partir des DT 1 et DT 2, caractérisez les éléments essentiels du système d'information et les conséquences possibles d'une compromission. Les termes vulnérabilité, menace, risque et incident doivent être employés avec précision.

**1.1** (1,5 point) Relevez deux actifs du système d'information qui présentent un enjeu important pour l'entreprise. 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.

**1.2** (1,5 point) 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.

**1.3** (1 point) Expliquez la différence entre une vulnérabilité et une menace, puis illustrez chaque terme par un élément distinct du dossier.

## PARTIE 2 : Diagnostiquer et hiérarchiser les risques (6 points)

***Analyse des vulnérabilités et cotation selon l'échelle fournie***

Utilisez exclusivement la méthode de cotation et les seuils du DT 2. Pour chaque risque étudié, appliquez la formule de criticité indiquée dans ce document et justifiez les valeurs de vraisemblance et d'impact retenues.

**Synthèse des vulnérabilités relevées dans le dossier**

| Repère | Constat | Actif principalement concerné |
|---|---|---|
| V1 | Accès distant d'administration sans authentification multifacteur | Passerelle VPN |
| V2 | SMBv1 actif sur le serveur de fichiers et absence de sauvegarde immuable | Serveur de fichiers |
| V3 | Règle du réseau Wi-Fi invité permettant un accès au réseau des postes internes | Réseau interne |
| V4 | SNMPv2 configuré avec une communauté par défaut | Commutateur cœur de réseau |

*Éléments techniques extraits des DT 1 à DT 3.*

**2.1** (2 points) Pour V1 et V2, déterminez une vraisemblance, un impact et une criticité. Présentez les calculs sous la forme $C = V \times I$, en utilisant les échelles du DT 2, puis indiquez la classe de criticité obtenue.

**2.2** (2 points) Complétez le tableau du DR 1 pour V1 à V4 : actif, vulnérabilité, scénario de risque, valeurs de vraisemblance et d'impact, criticité et classe. Les scénarios doivent décrire une conséquence plausible, sans présenter comme avéré un incident qui n'est pas démontré par le dossier.

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

## PARTIE 3 : Proposer un plan de remédiation opérationnel (6 points)

***Choix des mesures, priorisation et vérification de leur efficacité***

Les remédiations doivent être proportionnées aux risques, compatibles avec les informations du dossier et formulées de façon compréhensible pour un responsable non spécialiste. Distinguez, lorsque cela est utile, la réduction de la vulnérabilité, la limitation des conséquences et la détection.

**3.1** (2 points) 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 permettant de limiter les interruptions de service ou les erreurs de configuration.

**3.2** (2 points) Proposez une remédiation pour V3 et une pour V4. Pour chacune, indiquez un test simple permettant de vérifier que la correction est effective.

**3.3** (2 points) Complétez le DR 2 avec un plan de traitement comprenant au moins trois actions. Pour chaque action, précisez une priorité, un responsable fonctionnel parmi les rôles disponibles dans le DT 2, une échéance cohérente avec la criticité et un indicateur de vérification. Faites apparaître une mesure de sauvegarde et de restauration.

## PARTIE 4 : Communiquer et respecter les obligations de sécurité (4 points)

***Sensibilisation des utilisateurs et conduite à tenir en cas d'incident***

La direction souhaite recevoir des recommandations directement applicables. Toute communication doit distinguer les faits constatés des hypothèses et ne pas exposer inutilement des informations techniques sensibles.

**4.1** (1,5 point) Rédigez un message de sensibilisation de deux ou trois phrases à destination des salariés concernant les accès distants et les demandes inhabituelles de validation de connexion. Le message doit indiquer un comportement attendu et un canal de signalement.

**4.2** (1,5 point) 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 règlement général sur la protection des données peut s'appliquer, ainsi que le délai prévu par ce règlement.

**4.3** (1 point) Donnez un indicateur mesurable permettant à la direction de suivre l'amélioration de la sécurité après la mise en œuvre des remédiations. Définissez ce que cet indicateur mesure.

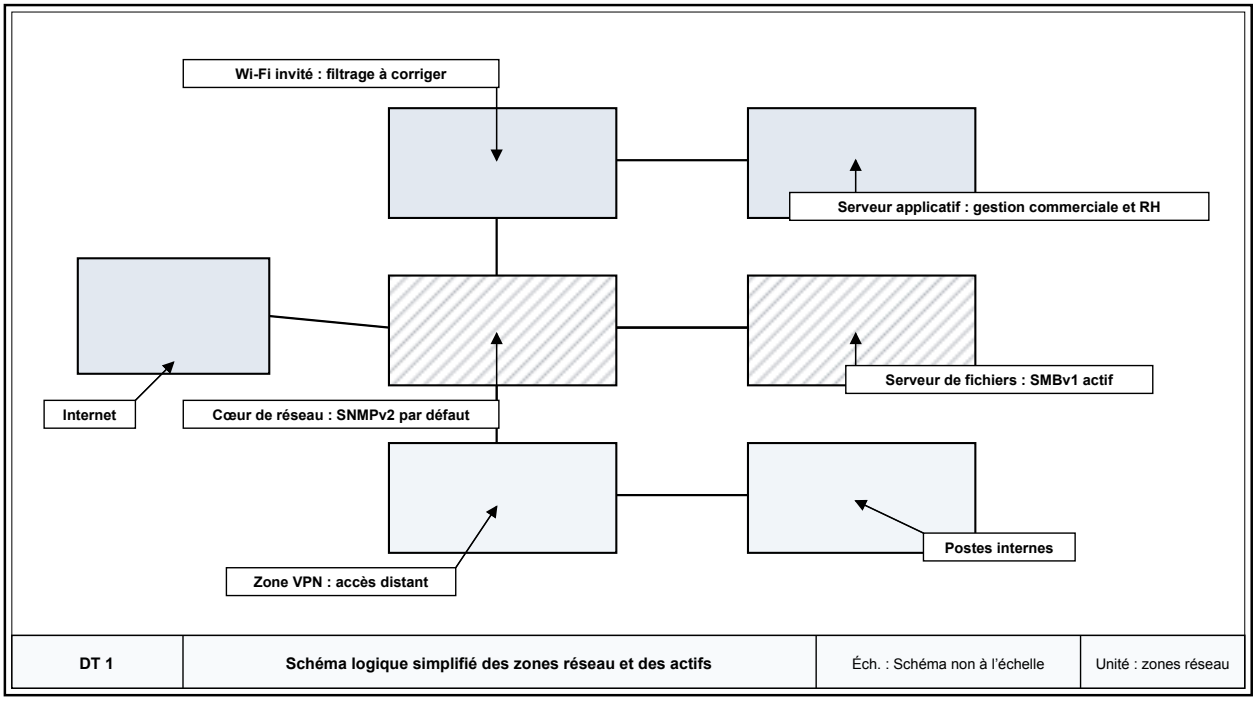
# DOSSIER TECHNIQUE ET RESSOURCES

Documents ressources nécessaires à la résolution du sujet

## **DT 1** : ARCHITECTURE SIMPLIFIÉE DU SYSTÈME D'INFORMATION

Le schéma représente les principaux équipements concernés par l'étude. La passerelle VPN est accessible depuis Internet pour le télétravail. Les postes internes accèdent au serveur de fichiers et à l'application de gestion commerciale. Le réseau Wi-Fi invité est destiné aux visiteurs et ne doit pas permettre l'accès aux ressources internes. L'application RH est hébergée sur le serveur applicatif interne.

État relevé lors de l'inventaire : l'administration VPN ne demande qu'un mot de passe ; le serveur de fichiers accepte SMBv1 ; le réseau invité dispose d'une règle de filtrage autorisant l'accès au sous-réseau des postes ; le commutateur cœur répond en SNMPv2 avec la communauté configurée par défaut. Ces constats décrivent des configurations observées et ne prouvent pas qu'une exploitation a eu lieu.




## **DT 2** : INVENTAIRE, MÉTHODE DE COTATION ET RÈGLES DE TRAITEMENT

La méthode utilisée pour cette évaluation est une échelle interne simplifiée. Elle sert à comparer les risques décrits dans le dossier et ne constitue pas un score normalisé. La criticité se calcule par $C = V \times I$, où $V$ est la vraisemblance et $I$ l'impact.

Vraisemblance : 1 = rare, conditions d'exploitation peu réunies ; 2 = peu probable, plusieurs conditions nécessaires ; 3 = probable, exposition ou faiblesse exploitable dans des conditions réalistes ; 4 = très probable, exposition directe ou faiblesse facilement exploitable. Impact : 1 = gêne limitée sur un poste ; 2 = interruption limitée d'un service secondaire ; 3 = interruption significative ou exposition de données internes ; 4 = interruption majeure, perte importante de données ou atteinte potentielle à des données personnelles.

Classes : 1 à 3 = faible ; 4 à 7 = modérée ; 8 à 11 = élevée ; 12 à 16 = critique. Pour départager deux risques de même criticité, traiter d'abord celui dont l'impact est le plus élevé, puis celui qui concerne un actif exposé à Internet.

Rôles disponibles pour le plan d'action : administrateur systèmes et réseaux, responsable informatique, responsable de la protection des données. Échéances proposées : risque critique, action de réduction immédiate et correction planifiée sous 7 jours ; risque élevé, correction sous 30 jours ; risque modéré, correction sous 90 jours. Une mesure immédiate de limitation peut précéder la correction définitive.

**Inventaire des actifs et enjeux**

| Actif | Fonction | Données ou service | Enjeu principal |
|---|---|---|---|
| Passerelle VPN | Accès distant des salariés | Accès aux ressources internes | Disponibilité et contrôle d'accès |
| Serveur de fichiers | Partage de documents | Documents commerciaux et administratifs | Confidentialité, intégrité et disponibilité |
| Réseau Wi-Fi invité | Accès Internet des visiteurs | Aucune ressource interne nécessaire | Séparation des réseaux |
| Commutateur cœur | Interconnexion des réseaux internes | Configuration et fonctionnement du réseau | Disponibilité et intégrité de l'infrastructure |
| Serveur applicatif | Gestion commerciale et application RH | Données clients, salariés et opérations | Confidentialité, intégrité et disponibilité |

*Informations communiquées par le responsable informatique.*

**Échelle de cotation et seuils**

| Valeur | Vraisemblance | Impact |
|---|---|---|
| 1 | Rare | Gêne limitée sur un poste |
| 2 | Peu probable | Interruption limitée d'un service secondaire |
| 3 | Probable | Interruption significative ou exposition de données internes |
| 4 | Très probable | Interruption majeure, perte importante de données ou atteinte potentielle à des données personnelles |
| Criticité | 1 à 3 faible ; 4 à 7 modérée | 8 à 11 élevée ; 12 à 16 critique |

*Méthode interne à appliquer dans le présent sujet.*

## **DT 3** : EXTRAITS DE JOURNALISATION ET INFORMATIONS D'EXPLOITATION

Les extraits ci-dessous proviennent de la passerelle VPN et du système de supervision. Les horodatages sont ceux du serveur de journalisation, synchronisé avec l'heure locale. L'adresse 198.51.100.24 est utilisée ici comme adresse de documentation et ne permet pas d'identifier une personne réelle.

À la date de l'examen, aucun élément fourni ne confirme une extraction de données, une modification de fichiers ou une interruption de service. Les sauvegardes du serveur de fichiers sont quotidiennes sur un

NAS du même site ; aucun test de restauration n’est consigné depuis neuf mois et aucune copie immuable n’est inventoriée.

Extrait VPN : 14/02/2026 03:12 : échec d’authentification pour le compte m.dupont depuis 198.51.100.24. 14/02/2026 03:13 : échec d’authentification pour le même compte depuis la même adresse. 14/02/2026 03:14 : authentification réussie pour le compte m.dupont depuis cette adresse. Le salarié indique ne pas avoir travaillé à cette heure et n’a pas encore confirmé si une connexion était légitime.

**Événements et indices à examiner**

| Source | Événement ou constat | Interprétation à vérifier |
|---|---|---|
| VPN | Deux échecs puis une authentification réussie pour le même compte en trois minutes | Connexion légitime, erreur de saisie ou utilisation non autorisée du compte |
| Sauvegardes | Copie quotidienne sur NAS du même site ; aucun test de restauration consigné depuis neuf mois | Capacité réelle de restauration et vulnérabilité aux incidents affectant le site |
| Filtrage réseau | Le réseau invité peut joindre le sous-réseau des postes internes | Portée exacte de la règle et possibilité d’accès aux services internes |
| Supervision | Aucune alerte de transfert massif de fichiers fournie dans le dossier | Complétude et durée de conservation des journaux à contrôler |

*Extraits retranscrits des journaux et constats de l’inventaire.*

**NE RIEN ÉCRIRE DANS CETTE PARTIE**

**DR 1** : Document réponse à rendre : diagnostic et cotation des risques **À RENDRE AVEC LA COPIE**

Complétez les cellules marquées « ... ». Utilisez la formule et les échelles du DT 2. Les scénarios doivent rester formulés comme des risques possibles lorsque les faits ne démontrent pas qu'un incident s'est produit.

**Tableau d'analyse des vulnérabilités**

| Repère | Actif | Vulnérabilité constatée | Scénario de risque | V | I | C = V × I | Classe |
|---|---|---|---|---|---|---|---|
| V1 | ..... | ..... | ..... | ..... | ..... | ..... | ..... |
| V2 | ..... | ..... | ..... | ..... | ..... | ..... | ..... |
| V3 | ..... | ..... | ..... | ..... | ..... | ..... | ..... |
| V4 | ..... | ..... | ..... | ..... | ..... | ..... | ..... |

**Cadre réservé aux justifications, calculs complémentaires ou schémas du candidat :**

**NE RIEN ÉCRIRE DANS CETTE PARTIE**

**DR 2** : Document réponse à rendre : plan de remédiation et vérification **À RENDRE AVEC LA COPIE**

Complétez au moins trois lignes. Indiquez des actions réalisables, une priorité cohérente avec la cotation du DR 1, un rôle responsable choisi dans le DT 2, une échéance et un indicateur vérifiable. Faites figurer une action de sauvegarde et de restauration.

**Plan d'actions priorisé**

| Risque ou repère | Action de remédiation | Priorité | Responsable fonctionnel | Échéance | Indicateur ou test de vérification |
|---|---|---|---|---|---|
| ..... | ..... | ..... | ..... | ..... | ..... |
| ..... | ..... | ..... | ..... | ..... | ..... |
| ..... | ..... | ..... | ..... | ..... | ..... |
| ..... | ..... | ..... | ..... | ..... | ..... |

**Cadre réservé aux justifications, calculs complémentaires ou schémas du candidat :**

.....

.....

.....

.....

.....

.....

.....

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.