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 LA COMPÉTENCE C6.5 : SURVEILLER UN SYSTÈME D'INFORMATION SÉCURISÉ

SESSION 2026

Durée : 2 heures

| SPÉCIALITÉ / UNITÉ | COEFF |
|---|---|
| RÉSEAUX ET TÉLÉCOMMUNICATIONS, PARCOURS CYBERSÉCURITÉ | 3,0 INDICATIF |

Moyens de calculs et matériel autorisés :

**L'usage de calculatrice avec mode examen actif est autorisé. L'usage de calculatrice sans mémoire, « type collège », est 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 CAHIER DES CHARGES : ALPINA CONNECT, INTÉGRATEUR DE SERVICES NUMÉRIQUES, MEYLAN (ISÈRE)

Vous intervenez au sein de l'équipe de supervision d'Alpina Connect. Le client, la société fictive Vercors Équipements, exploite un système d'information composé d'un réseau bureautique, d'un serveur de fichiers, d'un serveur web exposé et d'un bastion d'administration. Les journaux sont centralisés dans une plateforme SIEM.

Votre mission consiste à examiner les données du dossier technique, qualifier une alerte, proposer une réponse proportionnée et formaliser les mesures de surveillance. Le repère « C10 » est une désignation locale d'évaluation ; l'intitulé national correspondant dans le BUT Réseaux et Télécommunications, parcours Cybersécurité, est la compétence C6.5 : « Surveiller un système d'information sécurisé ».

Les règles de conservation et de traitement des journaux indiquées dans le dossier sont celles retenues par l'entreprise pour ce cas. Toute proposition doit préserver la traçabilité, limiter l'accès aux données et éviter une interruption de service non justifiée.

## Partie 1 : Analyse fonctionnelle et cadrage de la surveillance (5 points)

***Identifier les actifs, les flux et les événements à surveiller***

À partir des documents DT 1 et DT 2, caractérisez le périmètre de surveillance et les événements utiles à la détection d'un incident.

**1.1** (2 points) Relevez quatre actifs du système d'information et indiquez, pour chacun, une conséquence possible sur la confidentialité, l'intégrité ou la disponibilité en cas de compromission. Appuyez vos réponses sur le rôle des actifs décrit dans le dossier.

**1.2** (1,5 point) À partir du schéma DT 1, identifiez les deux flux qui doivent être surveillés en priorité pour détecter une tentative d'administration non autorisée. Pour chacun, indiquez la source, la destination et le type d'événement à collecter.

**1.3** (1,5 point) Dans le tableau du DR 1, classez les trois événements du DT 2 en événement attendu, anomalie à vérifier ou incident probable. Justifiez chaque classement par un indice présent dans les données.

## Partie 2 : Exploitation des journaux et qualification d'une alerte (5 points)

***Calculer des volumes et corréler des événements***

Utilisez les seuils et les extraits de journaux du DT 2 ainsi que les paramètres de collecte du DT 3. Les calculs doivent faire apparaître les unités et les étapes utiles.

**Paramètres de collecte et seuils de détection**

| Paramètre | Valeur |
|---|---|
| Nombre moyen de journaux collectés | 12 000 événements par jour |
| Taille moyenne d'un événement stocké | 0,8 kB |
| Durée de conservation opérationnelle | 30 jours |
| Seuil d'alerte échecs SSH | 8 échecs ou plus en 5 minutes depuis une même adresse IP |
| Marge de stockage à réserver | 20 % du volume brut calculé |

*Données d'exploitation fournies par l'équipe SIEM.*

**2.1** (2 points) Calculez le volume brut de journaux généré en 30 jours, puis le volume de stockage à prévoir avec la marge de 20 %. Utilisez la relation $V = N \times s$, où $N$ est le nombre d'événements et $s$ leur taille moyenne. Donnez le résultat en kB puis en MB, avec $1\ \text{MB} = 1\,000\ \text{kB}$.

**2.2** (1,5 point) Dans le DT 2, comptez les échecs SSH provenant de 203.0.113.77 dans la fenêtre de 5 minutes indiquée. Comparez ce nombre au seuil d'alerte et concluez si la règle est déclenchée.

**2.3** (1,5 point) Corrélez les événements SSH et l'ouverture de session réussie du DT 2. Indiquez la chronologie, le compte concerné et le niveau de qualification le plus adapté parmi les choix suivants : événement attendu, anomalie à vérifier, incident probable. Justifiez votre choix avec au moins deux indices.

## Partie 3 : Préparation du traitement opérationnel (5 points)

***Établir une procédure de vérification et de réponse***

Vous êtes opérateur de supervision de premier niveau. Le DT 3 précise les moyens disponibles et les actions autorisées. Vous ne devez ni supprimer les journaux ni lancer d'action destructive.

**3.1** (2 points) Rédigez une séquence de quatre actions, dans l'ordre, pour vérifier et traiter l'incident probable repéré en partie 2. La séquence doit inclure la préservation des preuves, une vérification de périmètre et une escalade vers le responsable de sécurité.

**3.2** (1,5 point) Complétez le tableau du DR 2 avec les informations de qualification disponibles : horodatage, adresse source, compte ciblé, actif concerné et éléments de preuve à conserver. Inscrivez « non déterminé » lorsqu'une information ne figure pas dans le dossier.

**3.3** (1,5 point) Proposez une mesure de confinement immédiat et une mesure corrective durable. Pour chacune, précisez le risque réduit et une précaution permettant de limiter l'impact sur le service.

## Partie 4 : Prévention, sécurité et traçabilité (5 points)

***Sécuriser les pratiques de supervision et formaliser le compte rendu***

Les mesures proposées doivent être compatibles avec les règles d'exploitation et de protection des données indiquées dans le DT 3. Les journaux sont des éléments de preuve et leur accès doit rester maîtrisé.

**4.1** (2 points) À partir du DT 3, indiquez deux mesures de protection des journaux et expliquez comment chacune contribue à leur confidentialité ou à leur intégrité. Mentionnez également une mesure garantissant la traçabilité des accès à la plateforme SIEM.

**4.2** (1,5 point) Rédigez une consigne de surveillance comportant un critère de déclenchement, les informations à enregistrer dans le ticket et le destinataire de l'escalade. La consigne doit pouvoir être appliquée par un opérateur sans interprétation supplémentaire.

**4.3** (1,5 point) Rédigez un compte rendu synthétique de l'événement, en distinguant faits observés, hypothèse, actions à engager et informations restant à confirmer. N'affirmez pas qu'un système est compromis si les éléments fournis ne permettent pas de l'établir.

# DOSSIER TECHNIQUE ET RESSOURCES

Documents ressources nécessaires à la résolution du sujet

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

Le SI comprend un pare-feu périmétrique, un serveur web public, un réseau bureautique, un serveur de fichiers et un bastion d'administration. Les serveurs transmettent leurs journaux au collecteur SIEM par syslog sur le réseau de supervision. Les administrateurs accèdent aux serveurs via le bastion ; l'administration directe depuis le réseau bureautique est interdite par la politique interne.

Les adresses du schéma sont réservées à la documentation et ne désignent pas des équipements publics réels.

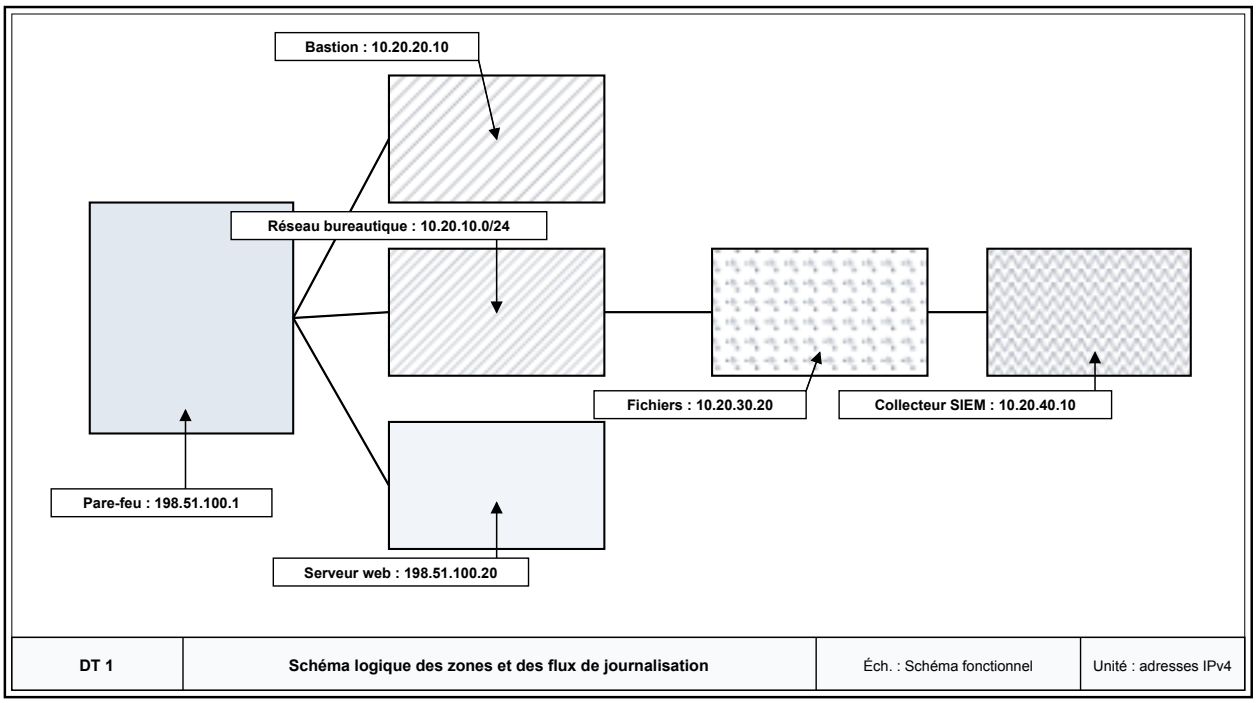



*Schéma fonctionnel, non à l'échelle. Les flèches représentent les flux autorisés décrits dans le dossier.*

**Actifs et journaux attendus**

| Actif | Adresse | Rôle | Journaux à centraliser |
|---|---|---|---|
| Serveur web | 198.51.100.20 | Publication du portail client | Authentification, serveur web, système |
| Bastion | 10.20.20.10 | Point d'accès d'administration | SSH, authentification, sessions administrateur |
| Serveur de fichiers | 10.20.30.20 | Stockage des dossiers internes | Authentification, accès aux fichiers, système |
| Collecteur SIEM | 10.20.40.10 | Centralisation et corrélation | Réception syslog, accès à la console, règles d'alerte |
| Pare-feu | 198.51.100.1 | Filtrage entre Internet et les zones internes | Connexions autorisées et refusées |

*Inventaire transmis par l'équipe d'exploitation.*

## **DT 2** : EXTRAIT HORODATÉ DES ÉVÉNEMENTS ET RÈGLE DE DÉTECTION

Les horodatages ci-dessous sont synchronisés par NTP et exprimés en heure locale. Les événements sont issus de journaux centralisés. Pour la question 2.2, la fenêtre d'analyse est de 09:00:00 à 09:04:59 inclus. La règle SIEM déclenche une alerte à partir de 8 échecs SSH en 5 minutes depuis une même adresse source.

**Extrait des événements reçus par le SIEM**

| Horodatage | Source | Actif ou service | Compte | Événement | Résultat |
|---|---|---|---|---|---|
| 09:00:12 | 203.0.113.77 | Bastion, SSH | admin | Échec d'authentification | Refusé |
| 09:00:41 | 203.0.113.77 | Bastion, SSH | admin | Échec d'authentification | Refusé |
| 09:01:03 | 203.0.113.77 | Bastion, SSH | admin | Échec d'authentification | Refusé |
| 09:01:38 | 203.0.113.77 | Bastion, SSH | admin | Échec d'authentification | Refusé |
| 09:02:05 | 203.0.113.77 | Bastion, SSH | admin | Échec d'authentification | Refusé |
| 09:02:31 | 203.0.113.77 | Bastion, SSH | admin | Échec d'authentification | Refusé |
| 09:03:14 | 203.0.113.77 | Bastion, SSH | admin | Échec d'authentification | Refusé |
| 09:04:02 | 203.0.113.77 | Bastion, SSH | admin | Échec d'authentification | Refusé |
| 09:04:26 | 203.0.113.77 | Bastion, SSH | admin | Ouverture de session | Réussie |
| 09:05:10 | 10.20.10.45 | Serveur de fichiers, SMB | j.martin | Connexion au partage commun | Réussie |
| 09:07:32 | 10.20.20.10 | Serveur de fichiers, SSH | svc-backup | Connexion planifiée de sauvegarde | Réussie |

*Données fournies pour l'analyse de l'incident.*

**DT 3** : PARAMÈTRES D'EXPLOITATION, CONSERVATION ET RÉPONSE À INCIDENT

La plateforme collecte en moyenne 12 000 événements par jour. La taille moyenne après normalisation et stockage est de 0,8 kB par événement. La conservation opérationnelle est fixée à 30 jours ; une marge de stockage de 20 % est réservée. Pour les conversions, utiliser $1\ \mathrm{MB} = 1\,000\ \mathrm{kB}$.

La procédure interne impose les règles suivantes : préserver l'horodatage et les identifiants des événements ; consigner toute action dans un ticket ; limiter l'accès aux journaux aux personnes habilitées ; conserver une copie des éléments utiles dans un espace à accès restreint ; faire valider par le responsable de sécurité toute mesure susceptible d'interrompre un service. L'opérateur de premier niveau peut enrichir l'alerte, vérifier les journaux et demander une escalade. Il ne peut pas supprimer des journaux, réinitialiser seul un compte administrateur ni modifier une règle de filtrage en production.

La politique interne prévoit l'authentification multifacteur pour les comptes d'administration, la restriction de l'accès SSH au bastion et la revue périodique des comptes de service.

**Actions de réponse et limites d'habilitation**

| Action | Autorisation opérateur de premier niveau | Condition ou précaution |
|---|---|---|
| Rechercher les événements associés et exporter les éléments utiles | Autorisée | Noter l'heure, l'auteur de l'export et l'emplacement sécurisé |
| Bloquer une adresse au pare-feu de production | Non autorisée seul | Demander validation au responsable de sécurité et à l'exploitation |
| Désactiver un compte administrateur | Non autorisée seul | Escalade immédiate et vérification de l'impact |
| Créer ou compléter un ticket d'incident | Autorisée | Séparer les faits observés des hypothèses |
| Supprimer ou modifier les journaux sources | Interdite | Préserver la valeur probante et la traçabilité |

*Extrait de la procédure interne applicable au scénario.*

**NE RIEN ÉCRIRE DANS CETTE PARTIE**

**DR 1** : Document réponse à rendre avec la copie : Questions 1.3 et 2.2 **À RENDRE AVEC LA COPIE**

Complétez directement les cellules marquées « ... ». Pour la justification, citez un indice précis des documents techniques.

**Classement des événements et vérification du seuil SSH**

| Événement ou constat | Classement ou résultat | Indice et justification |
|---|---|---|
| Connexion SMB de j.martin à 09:05:10 | ..... | ..... |
| Connexion SSH svc-backup à 09:07:32 | ..... | ..... |
| Échecs SSH depuis 203.0.113.77 | Nombre d'échecs : ... ; seuil déclenché : ... | ..... |

*Une ligne par événement ou constat demandé.*

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

.....

.....

.....

.....

.....

.....

.....

**NE RIEN ÉCRIRE DANS CETTE PARTIE**

**DR 2** : Document réponse à rendre avec la copie : Question 3.2 **À RENDRE AVEC LA COPIE**

Complétez les champs à partir des seuls éléments fournis dans le dossier technique. Inscrivez « non déterminé » si l'information n'est pas disponible.

**Fiche de qualification de l'alerte**

| Champ | Renseignement |
|---|---|
| Premier horodatage de la séquence | ..... |
| Dernier horodatage de la séquence | ..... |
| Adresse source | ..... |
| Compte ciblé | ..... |
| Actif concerné | ..... |
| Nombre d'échecs SSH observés | ..... |
| Événement de réussite observé | ..... |
| Éléments de preuve à préserver | ..... |
| Informations restant à confirmer | ..... |

*Renseigner les faits observés et les éléments de preuve à préserver.*

**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.