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 Réseaux et Télécommunications, parcours Cybersécurité

Session 2026 • Code sujet : **26-BUT-RT-EP1** • Durée : **2 heures** • Coefficient : **3,0**
indicatif

Sommaire

Cliquez sur une partie pour y accéder directement

1. **Analyse fonctionnelle et cadrage de la surveillance** (3 questions) — **Page 3**
2. **Exploitation des journaux et qualification d'une alerte** (3 questions) — **Page 5**
3. **Préparation du traitement opérationnel** (3 questions) — **Page 7**
4. **Prévention, sécurité et traçabilité** (3 questions) — **Page 10**
5. **Ce qu'il faut retenir & Questions fréquentes (FAQ)** (Synthèse & Q&A Examen) — **Page 12**

Sujet officiel (PDF) : https://butrt.fr/assets/annales/but-rt/C10 - Surveiller un système d'information sécurisé/2026/BUT Réseaux et Télécommunications - C10 - Surveiller un système d'information sécurisé - Session 2026 - 1-Sujet.pdf

1. Analyse fonctionnelle et cadrage de la surveillance

Dans le cadre de la supervision du système d'information de Vercors Équipements, il faut délimiter les actifs, les flux et les événements utiles à la détection d'incidents. L'analyse s'appuie sur l'architecture, l'inventaire des actifs et les journaux d'événements.

Actifs et conséquences d'une compromission

Question 1.1. 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.

Les rôles indiqués dans l'inventaire permettent de relier chaque actif aux impacts possibles d'une compromission sur la confidentialité, l'intégrité ou la disponibilité.

Actif	Rôle	Conséquence possible
Serveur web	Publication du portail client	Altération du portail ou exposition de données clients
Bastion	Point d'accès d'administration	Accès non autorisé aux serveurs
Serveur de fichiers	Stockage des dossiers internes	Divulgation ou modification des dossiers
Collecteur SIEM	Centralisation et corrélation des journaux	Altération des preuves ou interruption de la détection

Ces conséquences touchent respectivement les services exposés, les accès d'administration, les données internes et la surveillance du système.

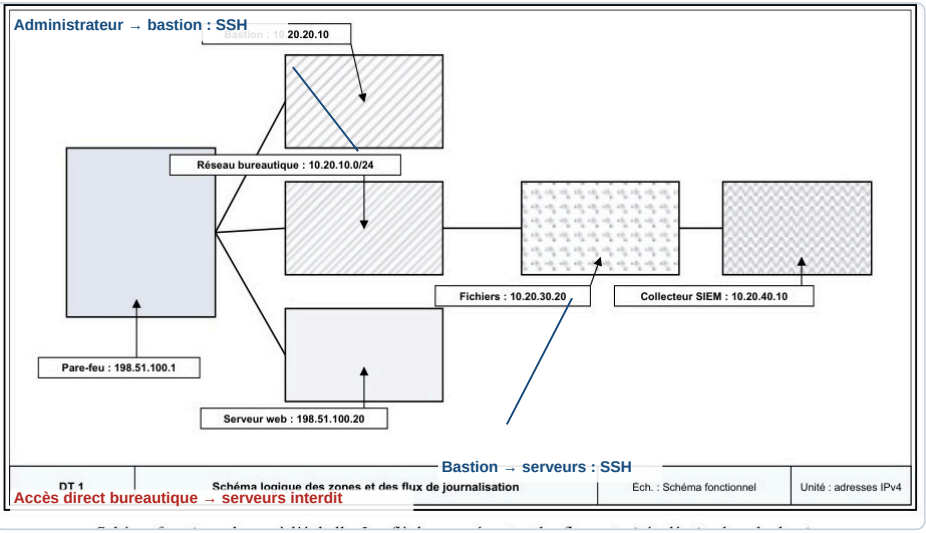
> ✓ **RÉPONSE À RETENIR**
>
> Serveur web : portail altéré ou données exposées. Bastion : accès aux serveurs. Fichiers : dossiers divulgués ou modifiés. SIEM : journaux altérés ou détection interrompue.

Flux prioritaires de surveillance

Question 1.2. À partir du schéma DT 1, identifiez les deux flux à surveiller en priorité pour détecter une tentative d'administration non autorisée. Pour chacun, indiquez la source, la destination et le type d'événement à collecter.

Les deux flux prioritaires suivent le chemin d'administration décrit dans DT 1 : l'administrateur se connecte d'abord au bastion, puis le bastion accède aux serveurs. L'adresse du poste source de l'administrateur n'est pas précisée. Pour les deux étapes, collecter les événements SSH, les échecs et réussites d'authentification ainsi que les ouvertures de sessions administrateur. L'accès direct du réseau bureautique aux serveurs étant interdit, tout événement correspondant doit être vérifié.

Flux d'administration à surveiller



✓ RÉPONSE À RETENIR

Administrateur → bastion 10.20.20.10 : authentifications SSH et sessions. Bastion 10.20.20.10 → serveurs : authentifications SSH et sessions administrateur. L'accès direct bureautique → serveurs est interdit.

Classement des événements

Question 1.3. Dans le tableau DR 1, classez les trois événements ou constats du DT 2 en événement attendu, anomalie à vérifier ou incident probable. Justifiez chaque classement en citant un indice précis présent dans les données.

La connexion SMB de j.martin est réussie vers le partage commun, sans indice d'accès anormal dans l'extrait : elle est classée comme événement attendu. La connexion SSH de svc-backup est également attendue, car le journal la décrit comme planifiée et indique qu'elle provient du bastion.

Les huit échecs SSH depuis la même adresse ciblent le compte admin et sont suivis d'une ouverture de session réussie à 09:04:26. Le seuil d'alerte est atteint : il s'agit d'un incident probable à traiter.

DR 1 complété : classement des événements

Événement ou constat	Attendu ent ou résultat	Succès au partage commun ion
Connexion SMB de j.martin à 09:05:10	..... Attendu	Connexion planifiée depuis le bastion
Connexion SSH svc-backup à 09:07:32	..... 8 ; oui	8 échecs en 5 min, puis session admin réussie .....
Échecs SSH depuis 203.0.113.77	Nombre d'échecs : ... ; seuil déclenché : ...	

✓ RÉPONSE À RETENIR

SMB j.martin : événement attendu. SSH svc-backup : événement attendu. SSH 203.0.113.77 : 8 échecs, seuil déclenché, puis réussite admin : incident probable.

2. Exploitation des journaux et qualification d'une alerte

L'épreuve fournit des paramètres de collecte et des journaux centralisés comprenant des échecs SSH, une ouverture de session réussie et d'autres connexions. Il faut calculer le stockage requis, vérifier le seuil d'alerte et corréler les événements pour qualifier la situation.

Calcul du volume de stockage

Question 2.1. 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 × s, où N est le nombre d'événements et s leur taille moyenne. Donnez les résultats en kB puis en MB, avec 1 MB = 1 000 kB, en faisant apparaître les unités et les étapes utiles.

La collecte représente **12 000 × 30 = 360 000 événements** sur 30 jours. Avec une taille moyenne de 0,8 kB par événement, le volume brut est **360 000 × 0,8 = 288 000 kB**. La conversion donne **288 000 ÷ 1 000 = 288 MB**. La marge de 20 % s'ajoute au volume brut : **288 000 × 1,20 = 345 600 kB**, soit **345 600 ÷ 1 000 = 345,6 MB**.

> ✓ **RÉPONSE À RETENIR**
>
> Volume brut : 288 000 kB, soit 288 MB. Stockage avec marge de 20 % : 345 600 kB, soit 345,6 MB.

Vérification du seuil SSH

Question 2.2. 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. Renseignez également le résultat dans le tableau DR 1.

Dans la fenêtre de 09:00:00 à 09:04:59, les échecs SSH depuis **203.0.113.77** surviennent à 09:00:12, 09:00:41, 09:01:03, 09:01:38, 09:02:05, 09:02:31, 09:03:14 et 09:04:02. Cela fait **8 échecs**. Le seuil est de 8 échecs ou plus en 5 minutes depuis une même adresse IP : il est donc atteint et l'alerte est déclenchée. Dans le DR 1, inscrire « 8 ; oui » et préciser que les huit échecs atteignent le seuil fixé.

DR 1 complété, résultat 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 : ... **8 ; oui**	**8 échecs en 5 min ; seuil atteint**

Une ligne par événement ou constat demandé

> ✓ **RÉPONSE À RETENIR**
>
> 8 échecs SSH en 5 minutes depuis 203.0.113.77 : seuil atteint, règle d'alerte déclenchée.

Corrélation et qualification de l’alerte

Question 2.3. 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 événement attendu, anomalie à vérifier ou incident probable. Justifiez votre choix avec au moins deux indices.

La séquence commence par huit échecs SSH sur le compte **admin** du bastion, depuis **203.0.113.77**, entre 09:00:12 et 09:04:02. À 09:04:26, la même adresse ouvre avec succès une session SSH pour ce compte. La qualification adaptée est **incident probable** : le nombre d’échecs atteint le seuil SIEM et une authentification réussit peu après les refus, avec la même source et le même compte ciblé. Ces faits justifient une vérification et une escalade, mais ne suffisent pas à établir que le système est compromis.

> **✓ RÉPONSE À RETENIR**
>
> Incident probable : huit échecs visant admin, puis session SSH réussie à 09:04:26 depuis la même adresse IP, 203.0.113.77.

3. Préparation du traitement opérationnel

L'opérateur de supervision de premier niveau doit traiter l'incident probable en respectant les limites d'habilitation et les consignes de conservation. Il prépare les preuves, vérifie le périmètre, renseigne la fiche de qualification et propose des mesures de réponse proportionnées.

Séquence de vérification et d'escalade

Question 3.1. Rédigez, dans l'ordre, une séquence de quatre actions pour vérifier et traiter l'incident probable repéré en partie 2. La séquence doit inclure la préservation des preuves, une vérification du périmètre et une escalade vers le responsable de sécurité. Respectez les actions autorisées et interdites à l'opérateur.

1. Exporter les journaux SSH utiles sans modifier les sources ; préserver horodatages et identifiants, puis noter l'heure, l'auteur et l'emplacement sécurisé de la copie.
2. Rechercher dans le SIEM et sur le bastion et les serveurs les événements associés, notamment les connexions et actions suivant l'ouverture de session réussie.
3. Créer ou compléter le ticket en séparant faits observés et hypothèses, puis escalader immédiatement au responsable de sécurité.
4. Proposer le blocage de l'adresse source et, si nécessaire, une mesure sur le compte ; faire valider toute action par les responsables habilités avant son application.

> **✓ RÉPONSE À RETENIR**
>
> Preuves préservées, périmètre vérifié, ticket renseigné et escalade faite ; confinement seulement après validation par les responsables habilités.

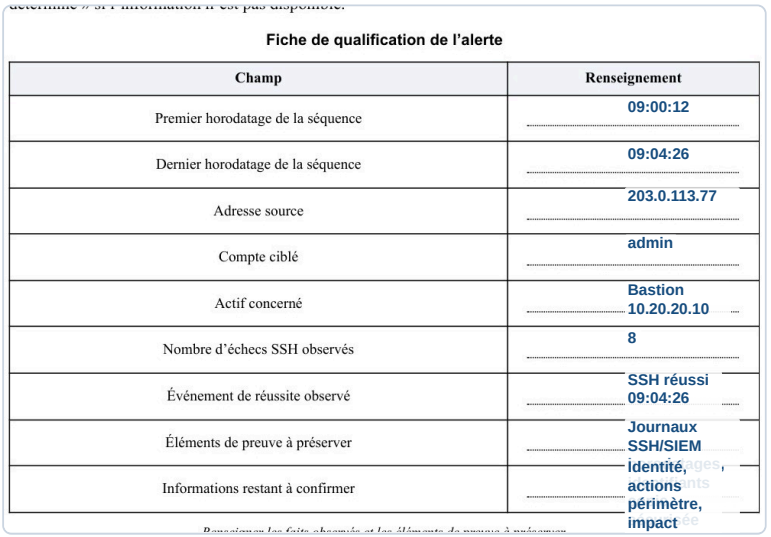
Fiche de qualification de l’alerte

Question 3.2. Complétez le tableau 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.

Champ	Renseignement
Premier horodatage de la séquence	09:00:12
Dernier horodatage de la séquence	09:04:26
Adresse source	203.0.113.77
Compte ciblé	admin
Actif concerné	Bastion, 10.20.20.10
Nombre d’échecs SSH observés	8
Événement de réussite observé	Ouverture de session SSH réussie à 09:04:26
Éléments de preuve à préserver	Journaux SSH et SIEM, horodatages et identifiants ; copie sécurisée avec heure et auteur de l’export
Informations restant à confirmer	Identité de l’auteur, actions après connexion, périmètre et impact

Les huit échecs visant le compte admin sont suivis d’une ouverture de session réussie depuis la même adresse sur le bastion. Les actions réalisées après connexion restent à vérifier.

DR 2 complété : fiche de qualification


Fiche de qualification de l’alerte

Champ	Renseignement
Premier horodatage de la séquence	09:00:12
Dernier horodatage de la séquence	09:04:26
Adresse source	203.0.113.77
Compte ciblé	admin
Actif concerné	Bastion 10.20.20.10
Nombre d’échecs SSH observés	8
Événement de réussite observé	SSH réussi 09:04:26
Éléments de preuve à préserver	Journaux SSH/SIEM
Informations restant à confirmer	Identité, actions, périmètre, impact

✓ RÉPONSE À RETENIR

203.0.113.77 : huit échecs visant admin, puis une session SSH réussie sur le bastion à 09:04:26.

Confinement et correction durable

Question 3.3. 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, en tenant compte des limites d'habilitation.

Confinement immédiat : demander au responsable de sécurité et à l'exploitation la validation d'un blocage temporaire de 203.0.113.77 au pare-feu. Cela réduit le risque de nouvelles tentatives ; vérifier d'abord qu'aucun accès légitime ne dépend de cette adresse. L'opérateur ne modifie pas seul le pare-feu en production.

Correction durable : faire appliquer la MFA aux comptes d'administration et restreindre l'accès SSH au bastion, conformément à la politique interne. Cela réduit le risque d'accès non autorisé ; planifier le déploiement avec validation, tests et maintien d'un accès de secours pour limiter l'impact sur le service.

> **✓ RÉPONSE À RETENIR**
>
> Blocage temporaire après validation ; appliquer durablement la MFA aux comptes d'administration et limiter SSH au bastion.

4. Prévention, sécurité et traçabilité

Cette partie porte sur la protection des journaux et la formalisation des pratiques de supervision conformément aux règles internes. Le candidat doit rédiger une consigne directement applicable et rendre compte de l'événement en distinguant les faits des hypothèses.

Protection des journaux et traçabilité

Question 4.1. 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.

Confidentialité : réserver l'accès aux journaux aux personnes habilitées et stocker les copies utiles dans un espace à accès restreint. **Intégrité :** ne pas supprimer ni modifier les journaux sources et préserver leurs horodatages et identifiants d'événements, afin de conserver leur valeur de preuve. Pour assurer la traçabilité, centraliser les journaux d'accès à la console SIEM, en conservant l'identité des utilisateurs et l'horodatage de leurs accès.

> ✓ **RÉPONSE À RETENIR**
>
> Accès réservé aux personnes habilitées ; copies en espace restreint ; journaux sources préservés ; accès à la console SIEM tracés.

Consigne de surveillance

Question 4.2. 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.

Consigne : déclencher une alerte dès qu'une même adresse source produit au moins 8 échecs SSH dans une fenêtre de 5 minutes. Créer ou compléter un ticket avec les horodatages, l'adresse source, le compte ciblé, l'actif concerné, le nombre d'échecs, les réussites associées et les identifiants des événements. Préserver les journaux ; pour tout export utile, noter l'heure, l'auteur et l'emplacement sécurisé. Escalader immédiatement au responsable de sécurité. Ne pas bloquer l'adresse ni désactiver un compte sans validation.

> ✓ **RÉPONSE À RETENIR**
>
> Déclenchement : au moins 8 échecs SSH en 5 minutes depuis une même adresse IP. Documenter les faits et preuves dans un ticket, puis escalader au responsable de sécurité.

Compte rendu de l’événement

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

Faits observés : l’adresse 203.0.113.77 a produit huit échecs SSH visant le compte admin sur le bastion, de 09:00:12 à 09:04:02, puis une ouverture de session réussie à 09:04:26. **Hypothèse :** tentative d’accès non autorisé suivie d’une authentification réussie ; la compromission n’est pas établie. **Actions :** préserver les journaux et leurs identifiants, vérifier les événements connexes et le périmètre atteint, puis transmettre le ticket au responsable de sécurité. **À confirmer :** légitimité de la connexion, identité de son auteur, activité de la session et éventuels actifs concernés.

> **✓ RÉPONSE À RETENIR**
>
> Huit échecs SSH suivis d’une connexion admin réussie sur le bastion : incident probable, compromission non établie. Préserver les preuves, vérifier le périmètre et escalader.

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

Bilan de l'épreuve : Épreuve du BUT Réseaux et Télécommunications, parcours Cybersécurité, session 2026, code 26-BUT-RT-EP1, d'une durée de 2 heures et de coefficient indicatif 3,0. À partir du SI de Vercors Équipements et d'une alerte SSH, elle évalue la surveillance des actifs, l'analyse et la corrélation de journaux, le dimensionnement du stockage, la réponse à incident et la traçabilité.

Notions-clés, formules & règles à maîtriser

- Le volume de journaux se calcule par V = N × s, puis la marge de stockage s'ajoute au volume brut.
- Le seuil SSH du sujet est atteint à partir de 8 échecs en 5 minutes depuis une même adresse IP.
- Une séquence d'échecs suivie d'une connexion réussie doit être corrélée et qualifiée selon les indices disponibles.
- La conservation des journaux exige de préserver leurs horodatages et identifiants, de restreindre les accès et de tracer les actions.

Points de vigilance & attentes du jury

- Précisez les actifs, adresses, sources, destinations et événements concernés plutôt que de décrire les flux de façon générale.
- Montrez les étapes de calcul, conservez les unités et appliquez la conversion 1 MB = 1 000 kB.
- Distinguez les faits des hypothèses et n'affirmez pas une compromission qui n'est pas établie par les journaux.
- Respectez les habilitations : ne supprimez ni ne modifiez les journaux et faites valider les actions à impact sur le service.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment calculer le volume de stockage nécessaire pour les journaux ?

Multipliez le nombre moyen d'événements quotidiens par 30, puis par la taille moyenne d'un événement pour obtenir le volume brut en kB. Ajoutez ensuite 20 % de marge et divisez par 1 000 pour convertir en MB.

Q : Quand la règle de détection des échecs SSH se déclenche-t-elle ?

Elle se déclenche lorsqu'au moins 8 échecs SSH sont observés en 5 minutes depuis une même adresse IP. Il faut compter uniquement les échecs dans la fenêtre indiquée, puis corréler les événements ultérieurs, notamment une éventuelle ouverture de session réussie.

Q : Que faire en premier lorsqu'une alerte SSH est qualifiée d'incident probable ?

Préservez les événements utiles et leurs horodatages, consignez les actions dans un ticket, vérifiez les journaux liés pour déterminer le périmètre, puis escaladez au responsable de sécurité. N'effectuez pas seul d'action interdite ou susceptible d'interrompre un service.

Q : Le sujet permet-il de conclure qu'un système est compromis après une connexion réussie ?

Non. Une ouverture de session après plusieurs échecs constitue un indice préoccupant et peut justifier la qualification d'incident probable, mais elle ne prouve pas à elle seule une compromission. Le compte, le périmètre et les activités réalisées restent à vérifier.

Sujet officiel associé (PDF) : https://butrt.fr/assets/annales/but-rt/C10 - Surveiller un système d'information sécurisé/2026/BUT Réseaux et Télécommunications - C10 - Surveiller un système d'information sécurisé - 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.