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

E6 : Valorisation de la donnée et cybersécurité

Session 2026 • Code sujet : **26-BTS-CIEL-E6** • Durée : **4 heures** • Coefficient : **4**

Sommaire

Cliquez sur une partie pour y accéder directement

1. Architecture réseau et adressage (4 questions) **Page 3**

2. Base de données et valorisation des données (3 questions) **Page 5**

3. Analyse d'incident et durcissement de la sécurité (4 questions) **Page 7**

4. Ce qu'il faut retenir & Questions fréquentes (FAQ) (Synthèse & Q&A Examen) **Page 9**

Sujet officiel (PDF) : https://coursbtsciel.fr/assets/annales/bts-ciel/E6 - Valorisation de la donnée et cybersécurité/2026/BTS CIEL - E6 - Valorisation de la donnée et cybersécurité - Session 2026 - 1-Sujet.pdf

1. Architecture réseau et adressage

Alpina Instruments dispose de quatre VLAN reliés par le commutateur de niveau 3 SW1, puis à Internet et au cloud par le routeur R1. À partir des besoins d'hôtes, de la topologie et du plan d'adressage, il faut dimensionner les sous-réseaux et compléter une table de routage.

Question 1.1. Pour chacun des quatre VLAN, proposer un préfixe IPv4 de longueur minimale permettant d'adresser le nombre d'hôtes demandé. Justifier chaque choix par le nombre d'adresses utilisables par sous-réseau, puis proposer, à partir du bloc 10.42.0.0/24, une allocation sans chevauchement en respectant l'ordre décroissant des besoins.

On choisit le plus petit sous-réseau offrant assez d'adresses utilisables, en réservant l'adresse réseau et l'adresse de diffusion. L'allocation suit l'ordre décroissant des besoins :

VLAN	Besoin	Préfixe minimal	Adresses utilisables	Allocation
10 Administration	50	/26	62	10.42.0.0/26
40 Wi-Fi invité	40	/26	62	10.42.0.64/26
20 Production	25	/27	30	10.42.0.128/27
30 Serveurs	12	/28	14	10.42.0.160/28

Les quatre sous-réseaux sont dans le bloc 10.42.0.0/24 et ne se chevauchent pas.

> ✓ **RÉPONSE À RETENIR**
>
> VLAN 10 : 10.42.0.0/26 ; VLAN 40 : 10.42.0.64/26 ; VLAN 20 : 10.42.0.128/27 ; VLAN 30 : 10.42.0.160/28.

Question 1.2. En respectant l'allocation du DT 1, déterminer pour le VLAN 20 le masque décimal, l'adresse réseau, l'adresse de diffusion, la plage des adresses utilisables et l'adresse de passerelle à configurer.

Le DT 1 attribue au VLAN 20 le réseau 10.42.0.128/27. Le masque /27 est 255.255.255.224 et le bloc contient 32 adresses, dont 30 utilisables. L'adresse réseau est .128 et l'adresse de diffusion .159. La première adresse utilisable est réservée à la passerelle.

Paramètre	Valeur
Masque	255.255.255.224
Adresse réseau	10.42.0.128
Adresse de diffusion	10.42.0.159
Plage utilisable	10.42.0.129 à 10.42.0.158
Passerelle	10.42.0.129

✓ RÉPONSE À RETENIR

Masque : 255.255.255.224 ; réseau : 10.42.0.128/27 ; diffusion : 10.42.0.159 ; plage utilisable : 10.42.0.129 à 10.42.0.158 ; passerelle : 10.42.0.129.

Question 1.3. Pour le serveur indiqué dans le DT 1, donner son adresse IPv6 complète, le préfixe de son sous-réseau et l'adresse IPv6 de passerelle correspondante. Expliquer en une phrase le rôle du préfixe /64.

SUP-01 appartient au VLAN 30, dont le préfixe IPv6 est `2001:db8:42:30::/64`. Son identifiant d'interface est `::20`, et la passerelle du VLAN se termine par `::1`. En IPv6 complet, l'adresse du serveur s'écrit `2001:0db8:0042:0030:0000:0000:0000:0020`. Le préfixe /64 identifie les 64 bits du réseau, les 64 bits restants identifiant l'interface.

✓ RÉPONSE À RETENIR

SUP-01 : 2001:db8:42:30::20/64 ; préfixe : 2001:db8:42:30::/64 ; passerelle : 2001:db8:42:30::1.

Question 1.4. Compléter dans le DR 1 la table de routage IPv4 du commutateur SW1. Pour les réseaux directement connectés, renseigner l'interface de sortie appropriée et, pour la route par défaut, indiquer le prochain saut donné par la topologie. Utiliser le format CIDR.

Les réseaux des VLAN et le réseau de transit sont directement connectés à SW1 : aucun prochain saut n'est requis. La route par défaut utilise comme prochain saut l'adresse de R1 sur le lien de transit. Les champs correspondants sont reportés sur le DR 1.

Table de routage IPv4 de SW1 complétée

Table de routage IPv4 de SW1 à compléter

Destination au format CIDR	Prochain saut	Interface de sortie
10.42.0.0/26	-	VLAN 10
10.42.0.64/26	-	VLAN 40
10.42.0.128/27	-	VLAN 20
10.42.0.160/28	-	VLAN 30
10.255.0.0/30	-	Lien de transit
0.0.0.0/0	10.255.0.1	Lien de transit

Compléter les champs marqués « ... ».

✓ RÉPONSE À RETENIR

Réseaux directement connectés : aucun prochain saut. Route par défaut 0.0.0.0/0 : prochain saut 10.255.0.1, interface Lien de transit.

2. Base de données et valorisation des données

La base de supervision regroupe les sites, les équipements et les événements associés, selon le schéma relationnel du DT 2. Les questions demandent d'écrire des requêtes SQL avec jointures, filtres temporels et agrégations, puis de donner un résultat à partir des enregistrements fournis.

Question 2.1. Écrire une requête SQL affichant, pour chaque site, son nom et le nombre d'événements de sévérité CRIT enregistrés le 18 février 2026 entre 00 h 00 inclus et le 19 février 2026 à 00 h 00 exclu. Utiliser les jointures nécessaires, filtrer sur la date et la sévérité, puis regrouper par site. Ne pas afficher les sites sans événement CRIT.

Les jointures relient chaque événement à son équipement, puis chaque équipement à son site. Les bornes temporelles incluent toute la journée du 18 février et excluent le 19 février. Le regroupement par identifiant et nom distingue les sites, et la jointure interne écarte ceux sans événement correspondant.

```
SELECT S.site_name, COUNT(E.event_id) AS nombre_evenements_crit
FROM Sites S
JOIN Devices D ON D.site_id = S.site_id
JOIN Events E ON E.device_id = D.device_id
WHERE E.severity = 'CRIT'
  AND E.event_time >= '2026-02-18 00:00:00'
  AND E.event_time < '2026-02-19 00:00:00'
GROUP BY S.site_id, S.site_name;
```

> ✓ **RÉPONSE À RETENIR**
>
> Décompte des événements CRIT du 18 février par site, sans afficher les sites dépourvus d'événement correspondant.

Question 2.2. À partir des données du DT 2, donner toutes les lignes du résultat exact de la requête de la question 2.1, sous la forme de deux colonnes nommées site_name et nombre_evenements_crit. Reporter les valeurs dans le DR 1.

Grenoble compte les quatre événements CRIT de AUTH-01 datés du 18 février. Chambéry compte un événement CRIT : celui de POSTE-17 à 11 h 21. Son autre événement CRIT, daté du 17 février à 23 h 58, est hors de l'intervalle demandé. Les événements WARN ne sont pas comptabilisés.

site_name	nombre_evenements_crit
Grenoble	4
Chambéry	1

Résultat SQL complété dans le DR 1

site_name	nombre_evenements_crit
Grenoble	4
Chambéry	1

✓ RÉPONSE À RETENIR

Grenoble : 4
Chambéry : 1

Question 2.3. Écrire une requête SQL affichant l'identifiant et le nom des équipements ayant généré au moins deux événements de sévérité CRIT le 18 février 2026. Regrouper par équipement, appliquer une condition d'agrégation et ne faire apparaître chaque équipement qu'une seule fois.

Le filtre conserve les événements CRIT du 18 février uniquement. Le regroupement par identifiant et nom rassemble les événements de chaque équipement. `HAVING` applique ensuite le seuil de deux événements après le comptage, et chaque équipement ne figure qu'une seule fois.

```
SELECT D.device_id, D.device_name
FROM Devices D
JOIN Events E ON E.device_id = D.device_id
WHERE E.severity = 'CRIT'
  AND E.event_time >= '2026-02-18 00:00:00'
  AND E.event_time < '2026-02-19 00:00:00'
GROUP BY D.device_id, D.device_name
HAVING COUNT(E.event_id) >= 2;
```

✓ RÉPONSE À RETENIR

Équipement retenu : D01, AUTH-01, avec quatre événements CRIT ce jour-là.

3. Analyse d’incident et durcissement de la sécurité

Les journaux du serveur d’authentification et du pare-feu montrent plusieurs échecs, une authentification réussie et un refus de trafic provenant de la même adresse IP. Il faut analyser cette séquence, proposer des mesures immédiates, renforcer les accès de service et d’administration et limiter l’impact d’un chiffrement malveillant.

Question 3.1. Reconstituer la chronologie des événements du DT 2 en distinguant les échecs d’authentification, l’authentification réussie et le refus du pare-feu. Identifier les éléments qui rendent cette séquence suspecte et préciser le compte concerné.

1. **09:12:04, 09:12:09 et 09:12:15 :** AUTH-01 journalise trois échecs pour `svc-backup`, depuis `203.0.113.77`.
2. **09:13:02 :** l’authentification réussit pour le même compte, depuis la même adresse.
3. **09:14:31 :** FW-01 refuse un trafic de cette adresse vers `10.42.0.170`.

Les échecs rapprochés suivis d’une réussite, puis d’une tentative vers un port sensible, rendent la séquence suspecte. Le compte concerné est `svc-backup`.

> **✓ RÉPONSE À RETENIR**
>
> Trois échecs, puis une authentification réussie de `svc-backup`, suivie d’un trafic TCP refusé vers `10.42.0.170:445`.

Question 3.2. Indiquer ce que permet de conclure l’événement DENY du pare-feu. Préciser la destination, le protocole et le port visés, puis expliquer pourquoi cet événement ne prouve pas à lui seul qu’une compromission a eu lieu.

L’événement `DENY` indique que FW-01 a bloqué une tentative provenant de `203.0.113.77` vers SUP-01, à l’adresse `10.42.0.170`. Le trafic visait le protocole TCP, port 445, utilisé notamment par SMB. Ce journal atteste le refus de cette communication, mais ne prouve pas qu’un accès ait réussi, ni qu’un système ait été modifié ou que des données aient été consultées. Il faut corréler cet événement avec les journaux du serveur et des autres équipements.

> **✓ RÉPONSE À RETENIR**
>
> FW-01 a refusé une tentative TCP vers le port 445 de SUP-01 (`10.42.0.170`). Ce refus ne prouve pas une compromission.

Question 3.3. Proposer trois mesures immédiates et complémentaires à prendre après la détection de cette séquence. Pour chacune, préciser l’objectif de sécurité visé parmi la confidentialité, l’intégrité, la disponibilité ou la traçabilité.

Prendre trois mesures complémentaires sans effacer les éléments utiles à l’enquête :

- **Confidentialité :** désactiver temporairement `svc-backup`, révoquer ses sessions et renouveler son secret.
- **Intégrité :** bloquer `203.0.113.77` et restreindre les accès SMB aux seuls hôtes autorisés afin de prévenir toute modification non autorisée.

- **Traçabilité :** préserver les journaux d'authentification, du pare-feu et de SUP-01 dans un stockage protégé, puis les examiner.

> **✓ RÉPONSE À RETENIR**
>
> Désactiver et sécuriser le compte, bloquer la source et restreindre SMB, puis préserver les journaux pour l'analyse.

Question 3.4. Proposer une configuration d'accès renforcée pour le compte de service svc-backup et pour les accès d'administration. Traiter le principe du moindre privilège, l'authentification, la gestion des secrets et la conservation des journaux. Préciser une mesure de sauvegarde limitant l'impact d'un chiffrement malveillant des données.

Accès	Configuration renforcée
`svc-backup`	Compte dédié non interactif, droits limités aux seules opérations de sauvegarde, accès réservé aux hôtes autorisés. Utiliser une identité de service gérée si possible ; sinon, conserver un secret long et unique dans un coffre, avec rotation.
Administration	Comptes nominatifs, moindre privilège, accès via bastion ou VPN et authentification multifacteur.
Journaux	Centralisation, accès restreint et conservation protégée contre l'altération.
Sauvegardes	Copies isolées ou immuables et tests réguliers de restauration.

Les identifiants de sauvegarde doivent être distincts des accès de production.

> **✓ RÉPONSE À RETENIR**
>
> Compte de service non interactif à privilèges minimaux, secrets protégés, MFA pour l'administration, journaux centralisés et protégés, sauvegardes isolées et testées.

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

Bilan de l'épreuve : L'épreuve E6 du BTS Cybersécurité, informatique et réseaux, électronique, session 2026, porte le code 26-BTS-CIEL-E6 et dure 4 heures, coefficient 4. Dans le contexte d'Alpina Instruments, elle évalue l'adressage et le routage IPv4/IPv6, l'exploitation de données de supervision par SQL, l'analyse de journaux d'incident et la proposition de mesures de cybersécurité.

Notions-clés, formules & règles à maîtriser

- Pour un sous-réseau IPv4 classique avec h bits d'hôte, le nombre d'adresses utilisables est 2^h - 2.
- Un préfixe IPv6 /64 identifie le sous-réseau et laisse 64 bits pour l'identifiant d'interface.
- Pour agréger des événements par site en SQL, joindre Sites, Devices et Events, filtrer les lignes puis utiliser GROUP BY et COUNT.
- La route par défaut IPv4 s'écrit 0.0.0.0/0 et envoie le trafic non couvert par une route plus spécifique vers le prochain saut.

Points de vigilance & attentes du jury

- Vérifier que chaque préfixe fournit assez d'adresses utilisables et que les sous-réseaux alloués ne se chevauchent pas.
- Distinguer l'adresse réseau, l'adresse de diffusion, la plage d'hôtes utilisables et l'adresse de passerelle.
- Pour filtrer une journée en SQL, inclure la borne de début et exclure le début du jour suivant.
- Un trafic refusé par le pare-feu établit qu'une tentative a été bloquée, pas qu'un système a été compromis.

Questions fréquentes sur cette épreuve (Q&A Examen)

Q : Comment choisir le préfixe IPv4 minimal pour un VLAN ?

Déterminez le nombre de bits h nécessaires pour que 2^h - 2 couvre le nombre d'hôtes demandé. Le préfixe vaut alors / (32 - h). Vérifiez ensuite l'alignement des réseaux et l'absence de chevauchement dans le bloc disponible.

Q : Comment filtrer en SQL les événements d'une journée entière ?

Utilisez une borne de début incluse et une borne de fin exclue : event_time est supérieur ou égal au début et inférieur au lendemain. Cette méthode couvre toute la journée et évite les problèmes liés aux fractions de seconde.

Q : Comment répartir le temps selon le barème de cette épreuve ?

Le sujet totalise 20 points : 7 en architecture et adressage, 6 en SQL et 7 en analyse d'incident. Répartissez votre temps selon ces pondérations et gardez quelques minutes pour relire vos calculs, filtres et réponses reportées dans le DR 1.

Q : Quels éléments faut-il couvrir dans les propositions de cybersécurité ?

Reliez les mesures aux objectifs demandés et distinguez les faits observés des hypothèses. Traitez le moindre privilège, l'authentification, la gestion des secrets, la conservation des journaux et des sauvegardes capables de limiter l'effet d'un chiffrement malveillant.

Sujet officiel associé (PDF) : https://coursbtsciel.fr/assets/annales/bts-ciel/E6 - Valorisation de la donnée et cybersécurité/2026/BTS CIEL - E6 - Valorisation de la donnée et cybersécurité - Session 2026 - 1-Sujet.pdf
Ressources BTS Cybersécurité, Informatique et réseaux, Électronique : 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.