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

BREVET DE TECHNICIEN SUPÉRIEUR

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE

ÉPREUVE E6 : VALORISATION DE LA DONNÉE ET CYBERSÉCURITÉ

SESSION 2026

Durée : 4 heures

SPÉCIALITÉ / UNITÉ	COEFF
CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE	4

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 INSTRUMENTS, ENTREPRISE DE CONCEPTION DE CAPTEURS INDUSTRIELS, GRENOBLE

Alpina Instruments exploite un système d'information réparti entre son site de Grenoble et une plateforme hébergée dans le cloud. Le réseau local comprend des postes administratifs, des postes de production, des serveurs internes et un réseau Wi-Fi invité. Un commutateur de niveau 3 assure le routage entre les VLAN. Un routeur relie le site à Internet et à la plateforme cloud.

À la suite d'alertes remontées par la supervision, l'équipe informatique doit vérifier le plan d'adressage, préparer des requêtes permettant de valoriser les données d'incidents et analyser des journaux de sécurité. Vous intervenez en appui de cette équipe. Les documents techniques DT 1 et DT 2 sont à utiliser pour répondre aux questions. Les réponses demandées dans le DR 1 sont à reporter directement dans ce document.

Le barème est de 20 points. Les réponses doivent être justifiées lorsque cela est demandé. Les adresses et noms de tables sont sensibles à la casse uniquement si le langage ou le système concerné l'exige.

PARTIE 1 : ARCHITECTURE RÉSEAU ET ADRESSAGE (7 points)

Analyser un plan d'adressage IPv4 et IPv6 et établir une table de routage

Le réseau local est décrit dans le DT 1. Le bloc IPv4 disponible pour les quatre VLAN est **10.42.0.0/24**. Les besoins en adresses d'hôtes sont indiqués dans le tableau du DT 1. Les adresses des interfaces de passerelle sont attribuées à la première adresse utilisable de chaque sous-réseau. Les adresses IPv6 des VLAN sont des préfixes de documentation et sont données dans le DT 1.

VLAN et besoins en adresses

VLAN	Usage	Nombre maximal d'hôtes à adresser
10	Administration	50
20	Production	25
30	Serveurs	12
40	Wi-Fi invité	40

Données de dimensionnement du réseau local

1.1 (2 points) Pour chacun des quatre VLAN, proposer un préfixe IPv4 de longueur minimale permettant d'adresser le nombre d'hôtes demandé. Justifier le choix à l'aide du nombre d'adresses utilisables par sous-réseau. À partir du bloc **10.42.0.0/24**, proposer une allocation sans chevauchement en respectant l'ordre de taille décroissante des besoins.

1.2 (2 points) En respectant l'allocation du DT 1, déterminer pour le VLAN 20 le masque décimal, l'adresse réseau, l'adresse de diffusion et la plage des adresses utilisables. Indiquer l'adresse de passerelle à configurer.

1.3 (1,5 point) Pour le serveur indiqué dans le DT 1, donner son adresse IPv6 complète et le préfixe de son sous-réseau. Indiquer l'adresse IPv6 de passerelle correspondante. Expliquer en une phrase le rôle du préfixe /64.

1.4 (1,5 point) Compléter dans le DR 1 la table de routage IPv4 du commutateur SW1. Pour les réseaux directement connectés, renseigner l'interface de sortie appropriée. Pour la route par défaut, renseigner le prochain saut indiqué par la topologie. Le format CIDR est attendu.

PARTIE 2 : BASE DE DONNÉES ET VALORISATION DES DONNÉES (6 points)

Écrire et exploiter des requêtes SQL avec jointure, agrégation et filtre

Le DT 2 présente le schéma relationnel et les enregistrements disponibles dans la base de supervision. Les horodatages sont exprimés en heure locale. Une ligne de la table **Events** représente un événement détecté par un équipement. Les identifiants de site et d'équipement relient les tables conformément au schéma fourni.

Schéma relationnel de la base de supervision

Table	Attributs
Sites	site_id, site_name
Devices	device_id, site_id, device_name
Events	event_id, device_id, event_time, severity, event_type

Tables et attributs disponibles dans le DT 2

2.1 (2 points) Écrire une requête SQL qui affiche, 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. La requête doit utiliser les jointures nécessaires, un filtre sur la date et la sévérité, puis un regroupement par site. Les sites sans événement CRIT ne sont pas à afficher.

2.2 (2 points) À partir des données du DT 2, donner le résultat exact de la requête demandée en 2.1 sous la forme de deux colonnes : **site_name** et **nombre_evenements_crit**. Indiquer toutes les lignes obtenues.

2.3 (2 points) Écrire une requête SQL qui affiche l'identifiant et le nom des équipements ayant généré au moins deux événements de sévérité **CRIT** le 18 février 2026. La requête doit utiliser un regroupement par équipement et une condition d'agrégation. Le résultat ne doit contenir chaque équipement qu'une seule fois.

PARTIE 3 : ANALYSE D'INCIDENT ET DURCISSEMENT DE LA SÉCURITÉ (7 points)

Interpréter des journaux, caractériser un incident et proposer des mesures de protection

Les extraits du DT 2 proviennent du serveur d'authentification et de l'équipement de filtrage du site. Les dates et heures sont synchronisées par le service NTP de l'entreprise. Les événements d'authentification

réussie ou échouée sont journalisés par le serveur. Les adresses IP privées observées sont attribuées aux équipements internes, sauf indication contraire dans les journaux.

Extrait des journaux de sécurité

Horodatage	Équipement	Événement	Détail
2026-02-18 09:12:04	AUTH-01	AUTH_FAIL	compte=svc-backup source=203.0.113.77
2026-02-18 09:12:09	AUTH-01	AUTH_FAIL	compte=svc-backup source=203.0.113.77
2026-02-18 09:12:15	AUTH-01	AUTH_FAIL	compte=svc-backup source=203.0.113.77
2026-02-18 09:13:02	AUTH-01	AUTH_SUCCESS	compte=svc-backup source=203.0.113.77
2026-02-18 09:14:31	FW-01	DENY	src=203.0.113.77 dst=10.42.0.170 proto=TCP dport=445

Extrait reproduit dans le DT 2

3.1 (2 points) 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 quel compte est concerné.

3.2 (1,5 point) 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.

3.3 (1,5 point) Proposer trois mesures immédiates et complémentaires à prendre après la détection de cette séquence. Pour chaque mesure, préciser l'objectif de sécurité visé parmi la confidentialité, l'intégrité, la disponibilité ou la traçabilité.

3.4 (2 points) Proposer une configuration d'accès renforcée pour le compte de service **svc-backup** et pour les accès d'administration. Votre réponse doit traiter le principe du moindre privilège, l'authentification, la gestion des secrets et la conservation des journaux. Préciser une mesure de sauvegarde permettant de limiter l'impact d'un chiffrement malveillant des données.

DOSSIER TECHNIQUE ET RESSOURCES

Documents ressources nécessaires à la résolution du sujet

DT 1 : TOPOLOGIE RÉSEAU ET PLAN D'ADRESSAGE

Le commutateur de niveau 3 SW1 assure le routage inter-VLAN. Les ports d'accès sont affectés au VLAN correspondant à l'équipement. Le lien entre SW1 et le routeur R1 est un lien de transit routé. R1 assure l'accès à Internet et à la plateforme cloud. La route par défaut de SW1 doit pointer vers R1.

Topologie : Internet et cloud sont reliés à R1. R1 est relié à SW1 par le réseau de transit **10.255.0.0/30**. L'adresse de R1 sur ce lien est **10.255.0.1/30** et celle de SW1 est **10.255.0.2/30**. SW1 relie les postes d'administration du VLAN 10, les équipements de production du VLAN 20, les serveurs du VLAN 30 et le point d'accès Wi-Fi invité du VLAN 40.

Le plan IPv4 du site attribue les sous-réseaux suivants : VLAN 10, **10.42.0.0/26**, passerelle **10.42.0.1** ; VLAN 40, **10.42.0.64/26**, passerelle **10.42.0.65** ; VLAN 20, **10.42.0.128/27**, passerelle **10.42.0.129** ; VLAN 30, **10.42.0.160/28**, passerelle **10.42.0.161**. Ces sous-réseaux sont inclus dans le bloc **10.42.0.0/24** et ne se chevauchent pas.

Les préfixes IPv6 sont les suivants : VLAN 10, **2001:db8:42:10::/64** ; VLAN 20, **2001:db8:42:20::/64** ; VLAN 30, **2001:db8:42:30::/64** ; VLAN 40, **2001:db8:42:40::/64**. Chaque passerelle IPv6 utilise l'adresse se terminant par **::1**. Le serveur de supervision SUP-01, dans le VLAN 30, utilise l'adresse **2001:db8:42:30::20/64**.

Interfaces et plan d'adressage du site

Équipement ou VLAN	Réseau IPv4	Passerelle ou adresse d'interface IPv4	Préfixe IPv6
VLAN 10 Administration	10.42.0.0/26	10.42.0.1	2001:db8:42:10::/64
VLAN 40 Wi-Fi invité	10.42.0.64/26	10.42.0.65	2001:db8:42:40::/64
VLAN 20 Production	10.42.0.128/27	10.42.0.129	2001:db8:42:20::/64
VLAN 30 Serveurs	10.42.0.160/28	10.42.0.161	2001:db8:42:30::/64
Lien R1-SW1	10.255.0.0/30	R1 : 10.255.0.1 ; SW1 : 10.255.0.2	Non configuré
SUP-01	10.42.0.170	10.42.0.161	2001:db8:42:30::20/64

Données de configuration de référence

Liens de la topologie logique

Équipement source	Équipement de destination	Rôle du lien
Internet et plateforme cloud	R1	Accès externe et filtrage périmétrique
R1	SW1	Lien de transit 10.255.0.0/30
SW1	Postes administratifs	Accès au VLAN 10
SW1	Équipements de production	Accès au VLAN 20
SW1	Serveurs, dont SUP-01	Accès au VLAN 30
SW1	Point d'accès Wi-Fi invité	Accès au VLAN 40

Description des connexions entre équipements

DT 2 : SCHÉMA DE BASE DE DONNÉES ET JOURNAUX D'INCIDENTS

La base de supervision comporte les tables suivantes. **Sites**(site_id, site_name), où **site_id** est la clé primaire. **Devices**(device_id, site_id, device_name), où **device_id** est la clé primaire et **site_id** une clé étrangère vers Sites. **Events**(event_id, device_id, event_time, severity, event_type), où **event_id** est la clé primaire et **device_id** une clé étrangère vers Devices. Les champs **event_time** et **severity** sont renseignés pour toutes les lignes fournies.

Les valeurs possibles de sévérité comprennent **INFO**, **WARN** et **CRIT**. Dans les questions SQL, les noms de tables et de colonnes doivent être repris tels qu'ils sont écrits dans ce document.

Contenu de la table Sites

site_id	site_name
1	Grenoble
2	Chambéry

Enregistrements disponibles dans la base de supervision

Contenu de la table Devices

device_id	site_id	device_name
D01	1	AUTH-01
D02	1	FW-01
D03	2	SUP-02
D04	2	POSTE-17

Enregistrements disponibles dans la base de supervision

Contenu de la table Events

event_id	device_id	event_time	severity	event_type
E001	D01	2026-02-18 09:12:04	CRIT	AUTH_FAIL
E002	D01	2026-02-18 09:12:09	CRIT	AUTH_FAIL
E003	D01	2026-02-18 09:12:15	CRIT	AUTH_FAIL
E004	D01	2026-02-18 09:13:02	CRIT	AUTH_SUCCESS
E005	D02	2026-02-18 09:14:31	WARN	FIREWALL_DENY
E006	D03	2026-02-18 10:08:20	WARN	DISK_THRESHOLD
E007	D04	2026-02-18 11:21:05	CRIT	MALWARE_QUARANTINE
E008	D04	2026-02-17 23:58:10	CRIT	MALWARE_QUARANTINE

Enregistrements à utiliser pour les questions SQL

Extrait des journaux bruts

Horodatage	Équipement	Événement	Détail
2026-02-18 09:12:04	AUTH-01	AUTH_FAIL	compte=svc-backup source=203.0.113.77
2026-02-18 09:12:09	AUTH-01	AUTH_FAIL	compte=svc-backup source=203.0.113.77
2026-02-18 09:12:15	AUTH-01	AUTH_FAIL	compte=svc-backup source=203.0.113.77
2026-02-18 09:13:02	AUTH-01	AUTH_SUCCESS	compte=svc-backup source=203.0.113.77
2026-02-18 09:14:31	FW-01	DENY	src=203.0.113.77 dst=10.42.0.170 proto=TCP dport=445

Journaux d'authentification et de filtrage correspondant aux événements du 18 février 2026

NE RIEN ÉCRIRE DANS CETTE PARTIE

DR 1 : Table de routage de SW1 et résultats SQL — **À RENDRE AVEC LA COPIE**

Compléter directement les cellules signalées par « ... ». Pour la table de routage, indiquer le prochain saut lorsqu'il existe et l'interface de sortie. Pour les résultats SQL, reporter les valeurs obtenues à la question 2.2.

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	.....	Lien de transit

Compléter les champs marqués « ... »

Résultat de la requête SQL de la question 2.2

site_name	nombre_evenements_crit
.....	.....
.....	.....

Reporter une ligne par site affiché par la requête

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.