Nom : _____ Date : _____ Note : _____

Architecture Zero Trust et sécurité

Vérification continue, micro-segmentation du réseau, gestion des identités et des accès, moindre privilège et contrôles de conformité.

SÉCURITÉ ZERO TRUST : PRÉSENTATION

SÉCURISÉ
CHIFFREMENT DES DONNÉES
Norme AES 256 bits

CONFORME
NORMES MONDIALES
Cadres RGPD (GDPR) et CCPA

ZERO TRUST
POLITIQUE D'ACCÈS
Authentification multifacteur

Bienvenue ! Ce dossier d'activités vous guide à travers l'architecture et la sécurité Zero Trust. Vous étudierez la vérification continue, la micro-segmentation du réseau, la gestion des identités et des accès (IAM), le moindre privilège et l'audit des sessions.

POINTS DE CONTRÔLE DE LA FICHE

- [ ] **Parties 1-4 : maîtrisez la cybersécurité et la prévention des menaces.**
- [ ] **Parties 5-7 : résolvez les mots croisés et les mots mêlés.**
- [ ] **Parties 8-9 : résolvez les études de cas et le défi de déchiffrement.**
- [ ] **Partie 10 : consultez les FAQ de base et avancées.**
- [ ] **Partie 11 : découvrez 10 faits concrets intéressants.**
- [ ] **Bonus : défi Réflexion rapide.**

Ouvrir le guide VPN.com de la cybersécurité

URL: https://www.vpn.com/fr/cybersecurite/securite-zero-trust/

Votre parcours d'apprentissage : stratégie Zero Trust

- Comprendre le principe fondamental de la vérification continue.
- Mettre en œuvre la micro-segmentation du réseau et l'accès selon le principe du moindre privilège.
- Configurez des contrôles de conformité des appareils et l'audit des sessions actives.

GUIDE DE SÉCURITÉ ZERO TRUST : CONSIGNES

Répondez aux questions à choix multiple et vrai/faux, complétez les phrases à trous à l'aide de la banque de mots, associez les définitions et résolvez les mots croisés et les mots mêlés. Appliquez vos connaissances à l'architecture Zero Trust. Terminez par l'activité bonus Réflexion rapide.

ARCHITECTURE ZERO TRUST ET SÉCURITÉ (INTRODUCTION)

La sécurité Zero Trust remplace les anciens modèles de périmètre réseau par une politique stricte : 'ne jamais faire confiance, toujours vérifier'. La mise en œuvre de la micro-segmentation, de la gestion des identités et des accès (IAM), du principe du moindre privilège et des contrôles de posture bloque les déplacements latéraux des menaces.

LISEZ ATTENTIVEMENT CHAQUE POINT DE CONTRÔLE ET CHOISISSEZ OU ÉCRIVEZ LA BONNE RÉPONSE.

Point de contrôle 1 : Défi QCM

1. Quel est le principe fondamental de la sécurité Zero Trust ?

- A. Ne jamais faire confiance, toujours vérifier chaque demande d'accès, quelle qu'en soit la source
- B. Considérer que tout le trafic situé derrière le pare-feu de l'entreprise est sûr
- C. Stocker les fichiers de base de données sans chiffrement pour gagner en vitesse
- D. Imposer l'authentification des e-mails uniquement avec des enregistrements SPF

2. Qu'est-ce que la micro-segmentation du réseau ?

- A. Diviser les réseaux en petites zones isolées pour contenir les déplacements latéraux
- B. Chiffrer les cartes réseau pendant le transit des données
- C. Connecter tous les serveurs locaux à une seule adresse IP publique
- D. Surveiller les frappes au clavier des utilisateurs dans les sessions du navigateur

3. Qu'est-ce que le principe du moindre privilège ?

- A. Limiter les droits d'accès des utilisateurs au strict nécessaire pour leur travail
- B. Accorder par défaut tous les privilèges système à chaque utilisateur
- C. Autoriser les connexions anonymes aux serveurs de base de données de l'entreprise
- D. Configurer des routeurs Wi-Fi publics sans mot de passe

4. Qu'est-ce que la gestion des identités et des accès (IAM) ?

- A. Cadres de gestion des identités numériques et de contrôle des privilèges système
- B. Des utilitaires antivirus qui analysent les répertoires de fichiers locaux
- C. Un système de stockage de sauvegarde sur supports isolés (air gap)
- D. Un protocole de passerelle de messagerie qui rejette les domaines usurpés

5. Que signifie l'authentification continue ?

- A. Vérifier à plusieurs reprises l'identité de l'utilisateur et la posture de l'appareil pendant une session active
- B. Changer le mot de passe principal toutes les 10 minutes
- C. Hacher les enregistrements de la base de données avec plusieurs algorithmes
- D. Chiffrer les paquets réseau en transit avec des clés TLS

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. Le Zero Trust part du principe que tout le trafic à l'intérieur du pare-feu de l'entreprise est sûr.

- ○ Vrai
- ○ Faux

7 Question 7

7. La micro-segmentation limite la capacité des attaquants à se déplacer latéralement entre les serveurs internes.

- ○ Vrai
- ○ Faux

8 Question 8

8. Le moindre privilège accorde par défaut l'accès à tous les fichiers de la base de données.

- ○ Vrai
- ○ Faux

9 Question 9

9. La vérification continue contrôle l'état de l'appareil et les identifiants tout au long d'une session de connexion.

- ○ Vrai
- ○ Faux

10 Question 10

10. Adopter le Zero Trust réduit l'impact des identifiants d'entreprise compromis.

- ○ Vrai
- ○ Faux

Point de contrôle 3 : Insertion des termes clés

Lisez chaque phrase ci-dessous et complétez le blanc avec le terme correct de la banque de mots.

1. Exiger des identifiants à chaque point d'accès relève de la _____ continue.
2. Diviser le réseau de l'entreprise en zones minuscules s'appelle la micro- _____ .
3. Configurer les identités numériques et le contrôle d'accès fait appel à un système _____ .
4. Restreindre les autorisations des utilisateurs applique le principe du moindre _____ .
5. Évaluer l'état de santé des appareils connectés consiste à analyser la _____ des appareils.
6. Journaliser et examiner les sessions actives relève de l' _____ de sécurité.

BANQUE DE MOTS DE VOCABULAIRE

AUDIT IAM PARE-FEU POSTURE PRIVILÈGE ROUTEUR SEGMENTATION VÉRIFICATION

Écrivez vos réponses ici :

1.
2.
3.
4.
5.
6.

Point de contrôle 4 : Association de notions sur la sécurité

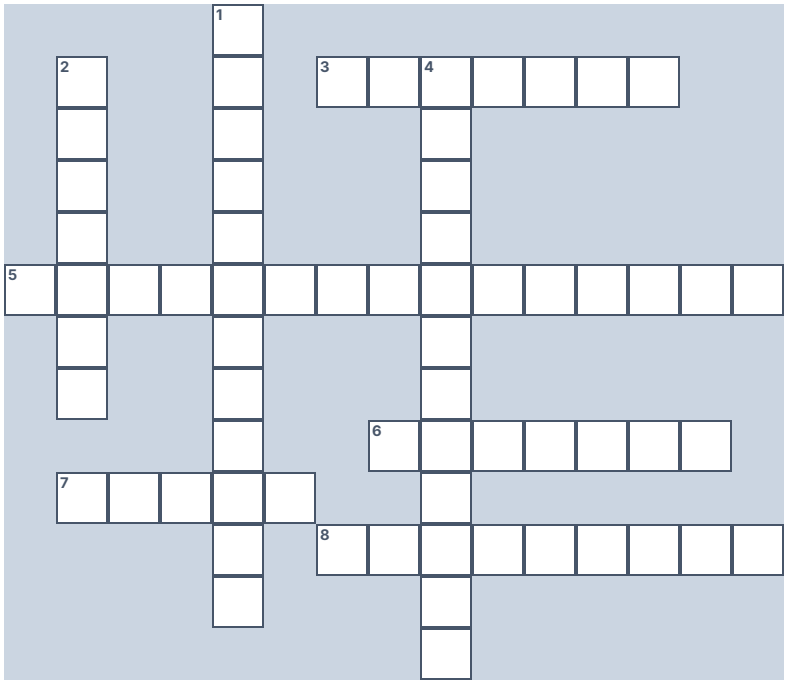
ASSOCIATION DE DÉFINITIONS

Associez chaque terme de vocabulaire à gauche à sa définition à droite en écrivant la lettre correspondante (A-H) dans la case à remplir.

☐	1. VÉRIFICATION	A	Gérer l'accès aux identifiants des utilisateurs.
☐	2. SEGMENTATION	B	Principe du moindre droit d'accès.
☐	3. IAM	C	Acheminement du trafic de paquets réseau.
☐	4. PRIVILÈGE	D	Protection par barrière réseau externe.
☐	5. CONFORMITÉ	E	Examen des sessions d'accès journalisées.
☐	6. AUDIT	F	Division des zones du réseau interne.
☐	7. PARE-FEU	G	Vérification constante des identifiants des utilisateurs.
☐	8. ROUTEUR	H	Évaluation de l'état de santé de l'appareil.

Point de contrôle 5 : Mots croisés

Résolvez la grille de mots croisés en tapant des lettres dans les cases blanches actives. Les numéros correspondent aux définitions ci-dessous.



HORIZONTALEMENT

3. Évaluation de l'état de santé des appareils. (7)

5. Administration des droits d'accès liés aux identifiants des utilisateurs (IAM). (15)

6. Protection par barrière réseau externe. (7)

7. Examen des sessions d'accès journalisées. (5)

8. Principe du droit d'accès minimal. (9)

VERTICALEMENT

1. Contrôle systématique des identifiants des utilisateurs. (12)

2. Acheminement du trafic des paquets réseau. (7)

4. Division du réseau interne en zones. (12)

Point de contrôle 5, variante : Définitions de mots croisés accessibles

Les utilisateurs de lecteurs d'écran et de clavier peuvent saisir les réponses des mots croisés directement dans les champs de texte ci-dessous.

HORIZONTALEMENT

3 horizontal: Évaluation de l'état de santé des appareils. (7 lettres):

5 horizontal: Administration des droits d'accès liés aux identifiants des utilisateurs (IAM). (15 lettres):

6 horizontal: Protection par barrière réseau externe. (7 lettres):

7 horizontal: Examen des sessions d'accès journalisées. (5 lettres):

8 horizontal: Principe du droit d'accès minimal. (9 lettres):

VERTICALEMENT

1 vertical: Contrôle systématique des identifiants des utilisateurs. (12 lettres):

2 vertical: Acheminement du trafic des paquets réseau. (7 lettres):

4 vertical: Division du réseau interne en zones. (12 lettres):

Point de contrôle 6 : Mots cachés

Trouvez les 8 termes de vocabulaire clés cachés dans la grille ci-dessous. Les mots peuvent être horizontaux, verticaux ou en diagonale.

P E C U B A Z G N D K A D O D

N G F H I D R E Q M V E I R Z

O E S F Q V F S A A E Q O N P

I L T X Q K R T U S R D N Y B

T I F S X W J I A R I Z Y Y L

A V G I M R J O M L F T O H Q

T I Q H R P Z N A O I V G U B

N R Y R O O Y D B H C L Z G J

E P O P U S N E W C A M U Z Y

M G Y O T T W S U K T V E A P

G B N V E U T A M G I V F U D

E Y U K U R R C B X O Z E D Y

S M R Q R E X C I P N D R I A

D J Q V W W L E J H T H A T G

B E I K T S V S R Z E H P E S

LISTE DE MOTS DE VOCABULAIRE

VERIFICATION SEGMENTATION GESTIONDESACCES PRIVILEGE POSTURE
AUDIT PAREFEU ROUTEUR

Point de contrôle 6, variante : Association de vocabulaire accessible

Associez chacun des 8 termes de vocabulaire de la grille de mots cachés à sa définition en écrivant la lettre (A-H) dans l'espace prévu.

TERMES DE VOCABULAIRE
A. VERIFICATION
B. SEGMENTATION
C. GESTIONDESACCES
D. PRIVILEGE
E. POSTURE
F. AUDIT
G. PAREFEU
H. ROUTEUR

DÉFINITIONS ET CHAMPS D'ASSOCIATION
1. Protection par barrière réseau externe.
2. Examen des sessions d'accès journalisées.
3. Principe du droit d'accès minimal.
4. Division du réseau interne en zones.
5. Acheminement du trafic des paquets réseau.
6. Évaluation de l'état de santé des appareils.
7. Administration des droits d'accès liés aux identifiants des utilisateurs (IAM).
8. Contrôle systématique des identifiants des utilisateurs.

Point de contrôle 7 : Défi des mots mélangés

Remettez les lettres ci-dessous dans l'ordre pour découvrir des notions et termes clés de la cybersécurité. Écrivez vos réponses dans les champs prévus.

1. T I A F E C I V O R N I
2. E O S N S D C G S E T A C E I
3. T P U E S R O
4. U A F E E P R
5. E I A T N G E T N S O M
6. G V R E L P I E I
7. I T A D U
8. O T R R U E U

Activité bonus : Réflexion rapide

3 RÉPONSES PAR CATÉGORIE. LE PREMIER À REMPLIR SA LISTE GAGNE.

1	Informations que vous ne devriez jamais partager			
2	Bonnes habitudes de sécurité à adopter dès aujourd'hui			
3	Choses vérifiées sur un appareil			
4	Choses qui sont journalisées			
5	Mots liés à la cybersécurité			
6	Choses que le Zero Trust vérifie			
7	Endroits où vous montrez une pièce d'identité au quotidien			
8	Façons de prouver que c'est bien vous			
9	Choses à faire après une fuite de données			
10	Signes qu'un ordinateur est infecté			
11	Raisons de mettre à jour les logiciels			
12	Niveaux d'accès dans une entreprise			
13	Outils de sécurité que vous connaissez			
14	Zones en lesquelles un réseau peut être divisé			
15	Proverbes sur la confiance			

Point de contrôle 8 : Études de cas sur la cybersécurité

Appliquez les notions apprises pour résoudre les scénarios réels ci-dessous.

ÉTUDE DE CAS 1 : PASSER À UNE ARCHITECTURE RÉSEAU ZERO TRUST

👷

Scénario : Une grande entreprise utilise actuellement un réseau interne plat, dans lequel n'importe quel appareil du réseau local peut accéder à tous les serveurs et bases de données de l'entreprise.

Question de discussion : Concevez une stratégie de micro-segmentation du réseau pour limiter les déplacements latéraux.

ÉTUDE DE CAS 2 : DÉPLOYER DES CONTRÔLES D'ACCÈS SELON LE MOINDRE PRIVILÈGE

👷

Scénario : Les journaux d'audit révèlent que des utilisateurs temporaires de la base de données et des employés de bas niveau disposent de droits globaux de lecture et d'écriture sur des bases de données comptables critiques.

Question de discussion : Auditez et restreignez les privilèges IAM de la base de données pour appliquer le principe du moindre privilège.

Point de contrôle 9 : Déchiffrer le code

Un professionnel de la cybersécurité protège les ressources réseau contre les acteurs malveillants en ligne. Utilisez la clé de correspondance lettres-chiffres ci-dessous pour déchiffrer le message en écrivant les lettres correspondantes dans les cases vides.

CLÉ DE CHIFFREMENT LETTRE-CHIFFRE

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

22	5	18	9	6	9	5	26		20	15	21	10	15	21	18	19
1	22	5	3		12	1		3	15	14	6	9	1	14	3	5
							26	5	18	15						

Message déchiffré :

ASTUCE : CHAQUE NOMBRE REPRÉSENTE LA POSITION DE LA LETTRE DANS L'ALPHABET (P. EX. 1 = A, 2 = B, 26 = Z).

Point de contrôle 10 : Questions fréquentes de base sur la cybersécurité (Partie A)

Passez en revue les questions et réponses courantes sur la réduction des menaces en ligne.

Q1: Qu'est-ce que le Zero Trust ?

Le Zero Trust est un cadre de sécurité qui part du principe que des menaces existent à la fois à l'extérieur et à l'intérieur du périmètre du réseau, et qui exige une vérification pour chaque requête. [1]

Q2: Quelle est la règle fondamentale du Zero Trust ?

Ne jamais faire confiance, toujours vérifier.

Q3: Qu'est-ce que la microsegmentation ?

Diviser un réseau en petits segments logiques sécurisés pour contrôler le trafic et contenir les intrusions.

Q4: Qu'est-ce que le principe du moindre privilège ?

Accorder aux utilisateurs uniquement les droits d'accès minimaux nécessaires à leurs tâches professionnelles. [2]

Q5: Que signifie IAM ?

Gestion des identités et des accès.

Point de contrôle 10 : Questions fréquentes de base sur la cybersécurité (Partie B)

Passez en revue les questions et réponses courantes sur la réduction des menaces en ligne.

Q6: En quoi le contrôle de conformité des appareils est-il utile ?

Il vérifie qu'un appareil est à jour, dispose d'un antivirus actif et est sécurisé avant d'autoriser l'accès.

Q7: Qu'est-ce que le mouvement latéral ?

Le processus qu'utilisent les attaquants pour se déplacer dans un réseau, d'un nœud initialement compromis vers des systèmes de plus grande valeur.

Q8: Le Zero Trust remplace-t-il les pare-feu ?

Non, il les renforce en ajoutant des vérifications centrées sur l'identité et des pare-feu de segmentation internes.

Q9: Qu'est-ce que l'authentification continue ?

Vérification continue de l'identité de l'utilisateur pendant toute la session active, et pas seulement à la connexion initiale.

Q10: Pourquoi un réseau plat est-il dangereux ?

Dans les réseaux plats, la compromission d'un seul nœud permet aux attaquants d'accéder facilement à n'importe quelle base de données du réseau.

Point de contrôle 10 : Questions fréquentes avancées sur la sécurité (Partie C)

Découvrez les aspects techniques avancés des cadres de sécurité, de l'analyse des logiciels malveillants et de la conformité des données.

Q1: Comment le Zero Trust répond-il aux limites du modèle périmétrique ?

Il remplace le modèle dépassé du « château fort et des douves », en déplaçant la défense du périmètre du réseau vers les identités des utilisateurs et les ressources elles-mêmes.

Q2: Qu'est-ce qu'un point de décision de politique (PDP) ?

Le composant du système qui évalue les demandes d'autorisation au regard des règles de sécurité pour décider si l'accès doit être accordé.

Q3: Qu'est-ce qu'un point d'application des politiques (PEP) ?

Le nœud du système (comme une passerelle ou un proxy) qui autorise ou bloque concrètement les demandes de connexion selon la décision du PDP.

Q4: Comment le contrôle d'accès basé sur les rôles (RBAC) soutient-il le Zero Trust ?

Le RBAC regroupe les autorisations en rôles précis, ce qui aide à éviter que les utilisateurs n'héritent de privilèges d'administration excessifs.

Q5: Qu'est-ce que le contrôle d'accès contextuel ?

Évaluer les demandes de connexion à l'aide d'indices secondaires comme la localisation géographique, la posture de l'appareil et l'heure de connexion pour estimer le risque.

Point de contrôle 10 : Questions fréquentes avancées sur la sécurité (Partie D)

Découvrez les aspects techniques avancés des cadres de sécurité, de l'analyse des logiciels malveillants et de la conformité des données.

Q6: En quoi la microsegmentation diffère-t-elle des VLAN classiques ?

Les VLAN divisent les réseaux en grands segments logiques à la couche 2, tandis que la micro-segmentation utilise des politiques logicielles pour isoler chaque charge de travail.

Q7: Qu'est-ce que l'accès juste à temps (JIT) ?

Accorder temporairement des droits d'administration élevés et les révoquer automatiquement une fois la tâche terminée.

Q8: Comment sécuriser les API dans un cadre Zero Trust ?

En exigeant des jetons OAuth signés cryptographiquement et en vérifiant les signatures des requêtes à chaque passerelle d'API.

Q9: Qu'est-ce qu'un client d'accès réseau zero trust (ZTNA) ?

Un agent logiciel qui établit des connexions sortantes sécurisées et chiffrées vers des applications précises plutôt que vers des sous-réseaux bruts.

Q10: Comment l'audit des journaux aide-t-il le Zero Trust ?

La journalisation continue permet aux outils d'analyse de sécurité automatisés de détecter les anomalies et de suspendre immédiatement les connexions malveillantes.

Partie 11 : 10 faits et enseignements concrets sur la cybersécurité

Découvrez des faits concrets sur les failles de sécurité, les mécanismes de défense et les normes de conformité.

1. APERÇU SÉCURITÉ

Les architectures Zero Trust remplacent l'ancien modèle du « château et des douves » par des règles de vérification centrées sur l'identité.

2. APERÇU SÉCURITÉ

La microsegmentation du réseau réduit la zone accessible aux logiciels malveillants en isolant les charges de travail dans de petites zones protégées.

3. APERÇU SÉCURITÉ

Le Zero Trust se concentre sur la protection des ressources, comme les actifs, les services et les comptes, plutôt que des segments de réseau. [1]

4. APERÇU SÉCURITÉ

Les politiques d'accès selon le principe du moindre privilège réduisent le risque de fuite de données des bases centrales par une menace interne.

5. APERÇU SÉCURITÉ

La validation de la posture des appareils vérifie en temps réel le niveau de correctifs du système d'exploitation et l'état de l'antivirus actif.

6. APERÇU SÉCURITÉ

Les courtiers ZTNA (Zero Trust Network Access) peuvent remplacer ou compléter les VPN d'entreprise pour restreindre l'étendue des accès des utilisateurs.

7. ZOOM SUR LA SÉCURITÉ

La délégation de privilèges d'administration à la demande (Just-In-Time, JIT) réduit le risque de vol d'identifiants sur les contrôleurs de domaine.

8. ZOOM SUR LA SÉCURITÉ

La validation continue journalise et audite le comportement des sessions, et suspend les utilisateurs dont les scripts s'exécutent de façon anormale.

9. ZOOM SUR LA SÉCURITÉ

Les défenses périmétriques traditionnelles ne bloquent pas les attaques latérales une fois qu'un identifiant administrateur a fuité.

10. APERÇU SÉCURITÉ

La publication spéciale NIST 800-207 (2020) donne une définition abstraite de l'architecture Zero Trust, avec des modèles de déploiement. [1]

Références techniques et sources

Le guide d'étude et les énigmes interactives sont tirés des normes internationales du NIST, de l'OWASP et de conformité en matière de protection des données.

RÉFÉRENCES ACADÉMIQUES ET PROFESSIONNELLES

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

[3] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

Corrigé : Point de contrôle 1 – Choix multiple

1 Question 1

Bonne réponse : A

NOTE PÉDAGOGIQUE

Quel est le principe fondamental de la sécurité Zero Trust ? → Ne jamais faire confiance, toujours vérifier chaque demande d'accès, quelle qu'en soit la source

2 Question 2

Bonne réponse : A

NOTE PÉDAGOGIQUE

Qu'est-ce que la micro-segmentation du réseau ? → Diviser les réseaux en petites zones isolées pour contenir les déplacements latéraux

3 Question 3

Bonne réponse : A

NOTE PÉDAGOGIQUE

Qu'est-ce que le principe du moindre privilège ? → Limiter les droits d'accès des utilisateurs au strict nécessaire pour leur travail

4 Question 4

Bonne réponse : A

NOTE PÉDAGOGIQUE

Qu'est-ce que la gestion des identités et des accès (IAM) ? → Cadres de gestion des identités numériques et de contrôle des privilèges système

5 Question 5

Bonne réponse : A

NOTE PÉDAGOGIQUE

Que signifie l'authentification continue ? → Vérifier à plusieurs reprises l'identité de l'utilisateur et la posture de l'appareil pendant une session active

Corrigé : Point de contrôle 2 – Vrai ou faux

6 Question 6

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : le Zero Trust n'accorde aucune confiance implicite fondée sur l'emplacement réseau, à l'intérieur comme à l'extérieur.

7 Question 7

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Vrai : de petites zones isolées limitent la distance qu'un intrus peut parcourir entre les serveurs.

8 Question 8

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : le moindre privilège n'accorde que l'accès minimal dont chaque rôle a besoin.

9 Question 9

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

La vérification continue contrôle l'état de l'appareil et les identifiants tout au long d'une session de connexion.

10 Question 10

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Adopter le Zero Trust réduit l'impact des identifiants d'entreprise compromis.

Corrigés du vocabulaire et grille d'évaluation

Grille de notation de l'enseignant : attribuez 1 point par association correcte (8 points au total) et par terme en contexte (6 points au total).

POINT DE CONTRÔLE 4 : CORRIGÉ DE L'ASSOCIATION DE NOTIONS

G 1. VÉRIFICATION	F 2. SEGMENTATION	A 3. IAM	B 4. PRIVILÈGE
H 5. CONFORMITÉ	E 6. AUDIT	D 7. PARE-FEU	C 8. ROUTEUR

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 VÉRIFICATION	2 SEGMENTATION	3 IAM	4 PRIVILÈGE
5 POSTURE	6 AUDIT		

POINT DE CONTRÔLE 6, VARIANTE : CORRIGÉ DE L'ASSOCIATION DE MOTS

1 G – PAREFEU	2 F – AUDIT	3 D – PRIVILEGE	4 B – SEGMENTATION
5 H – ROUTEUR	6 E – POSTURE	7 C – GESTIONDESACCES	8 A – VERIFICATION

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer VÉRIFICATION, SEGMENTATION et IAM avec leurs propres mots et donner un exemple pour chacun.

Études de cas :
Demandez aux élèves de justifier leurs recommandations par des faits tirés de la fiche plutôt que par des suppositions.

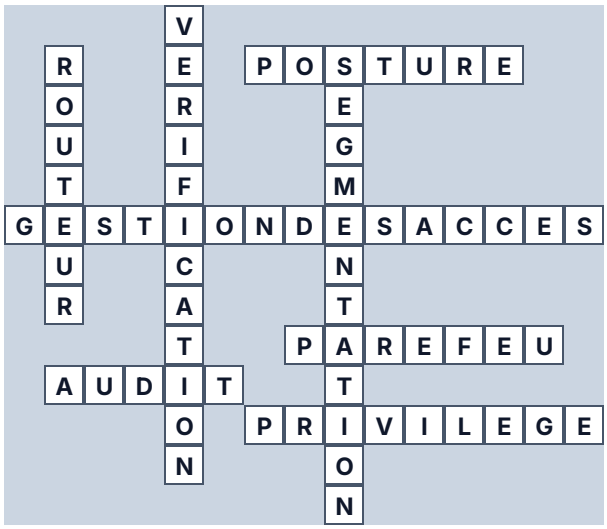
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

P	E	C	U	B	A	Z	G	N	D	K	A	D	O	D
N	G	F	H	I	D	R	E	Q	M	V	E	I	R	Z
O	E	S	F	Q	V	F	S	A	A	E	Q	O	N	P
I	L	T	X	Q	K	R	T	U	S	R	D	N	Y	B
T	I	F	S	X	W	J	I	A	R	I	Z	Y	Y	L
A	V	G	I	M	R	J	O	M	L	F	T	O	H	Q
T	I	Q	H	R	P	Z	N	A	O	I	V	G	U	B
N	R	Y	R	O	O	Y	D	B	H	C	L	Z	G	J
E	P	O	P	U	S	N	E	W	C	A	M	U	Z	Y
M	G	Y	O	T	T	W	S	U	K	T	V	E	A	P
G	B	N	V	E	U	T	A	M	G	I	V	F	U	D
E	Y	U	K	U	R	R	C	B	X	O	Z	E	D	Y
S	M	R	Q	R	E	X	C	I	P	N	D	R	I	A
D	J	Q	V	W	W	L	E	J	H	T	H	A	T	G
B	E	I	K	T	S	V	S	R	Z	E	H	P	E	S

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

3 horizontal: POSTURE Évaluation de l'état de santé des appareils. (7 lettres)

5 horizontal: GESTIONDESACCES Administration des droits d'accès liés aux identifiants des utilisateurs (IAM). (15 lettres)

6 horizontal: PAREFEU Protection par barrière réseau externe. (7 lettres)

7 horizontal: AUDIT Examen des sessions d'accès journalisées. (5 lettres)

8 horizontal: PRIVILEGE Principe du droit d'accès minimal. (9 lettres)

VERTICALEMENT

1 vertical: VERIFICATION Contrôle systématique des identifiants des utilisateurs. (12 lettres)

2 vertical: ROUTEUR Acheminement du trafic des paquets réseau. (7 lettres)

4 vertical: SEGMENTATION Division du réseau interne en zones. (12 lettres)

Corrigé des mots mélangés et du code

Corrigé de l'activité de remise en ordre des lettres du vocabulaire et du défi du code secret.

CORRIGÉ DES MOTS MÉLANGÉS

1. TIAFECIVORNI — **VERIFICATION**
2. EOSNSDCGSETACEI — **GESTIONDESACCES**
3. TPUESRO — **POSTURE**
4. UAFEEPR — **PAREFEU**
5. EIATNGETNSOM — **SEGMENTATION**
6. GVRELPIEI — **PRIVILEGE**
7. ITADU — **AUDIT**
8. OTRRUEU — **ROUTEUR**

CORRIGÉ DU DÉFI DU CODE SECRET

"VERIFIEZ TOUJOURS AVEC LA CONFIANCE ZERO"

Corrigé des études de cas

A Étude de cas 1 : Passer à une architecture réseau Zero Trust

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : une grande entreprise utilise actuellement un réseau interne plat où n'importe quel appareil du réseau local peut accéder à tous les serveurs et bases de données de l'entreprise.
- Stratégie et solution recommandées : segmentez le réseau plat en zones départementales isolées. Installez des pare-feu internes pour contrôler le trafic entre les zones et imposez la validation d'un jeton de connexion pour tout accès.

B Étude de cas 2 : Déployer des contrôles d'accès selon le moindre privilège

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : les journaux d'audit révèlent que des utilisateurs temporaires de la base de données et des employés de bas niveau disposent de droits globaux de lecture et d'écriture sur des bases de données comptables critiques.
- Stratégie et solution recommandées : révoquez tous les privilèges d'administration globaux. Mettez en place un contrôle d'accès basé sur les rôles (RBAC) correspondant exactement aux postes, et instaurez des revues automatisées hebdomadaires des autorisations.