
— DOSSIER SÉCURITÉ

Dossier sécurité Whiteboard

Hébergement, isolation, identité, chiffrement, continuité, sous-traitants, évaluation et cadre légal : les réponses à transmettre à votre RSSI, vérifiables dans le produit et sa documentation.

En une page

Hébergement	Hetzner Online GmbH, Allemagne (UE) ; au Maroc sur demande (instance dédiée).
Isolation	PostgreSQL, sécurité au niveau des lignes ENABLE + FORCE sur chaque table, rôle applicatif NOSUPERUSER NOBYPASSRLS.
Identité	SAML 2.0, OpenID Connect, Entra ID, Google ; SCIM 2.0 ; MFA TOTP imposable ; expiration d'inactivité réglable.
Traçabilité	Journal d'audit en ajout seul (déclencheur PostgreSQL), conservation de 1 à 10 ans.
Chiffrement	TLS + HSTS ; secrets chiffrés dans la base ; sauvegardes chiffrées AES-256 ; liens signés expirants.
Continuité	PITR pgBackRest ; exercice chronométré du 10/10/2026 ; objectifs RPO 15 min, RTO 4 h.
Réversibilité	Export complet : NDJSON, fichiers, cours IMS Common Cartridge.
Évaluation	Auto-évaluation interne OWASP ASVS 4.0.3 niveau 2 ; test d'intrusion externe planifié ; aucune certification revendiquée.

01 · HÉBERGEMENT

Un hébergeur nommé. Une option Maroc.

Hetzner, en Allemagne

Le service est hébergé par Hetzner Online GmbH, dans un centre de données en Allemagne, dans l'Union européenne.

Un déménagement écrit

La relocalisation est une procédure écrite et répétée : restauration sur les nouveaux serveurs, puis bascule DNS, lors d'une maintenance annoncée d'une à trois heures.

Au Maroc sur demande

La même image applicative tourne chez un hébergeur marocain : elle ne demande que des conteneurs, PostgreSQL et un stockage compatible S3. Instance dédiée, offre Entreprise.

Sans service propriétaire

Ni base de données gérée, ni file de messages d'un fournisseur cloud : files, cache et tâches tournent dans PostgreSQL. Rien ne vous attache à un hébergeur.

02 · ISOLATION

Chaque client est isolé par la base de données elle-même.

La plupart des plateformes mutualisées isolent leurs clients dans le code. Nous le faisons aussi, et PostgreSQL le garantit en dessous.

Sécurité au niveau des lignes, forcée

Chaque table porte l'identifiant de l'organisation, avec ENABLE et FORCE ROW LEVEL SECURITY : une politique refuse toute ligne d'une autre organisation, même au propriétaire des tables.

✓ **Prouvé à chaque livraison**

Un test automatique échoue si une table n'est pas protégée ou si une lecture croisée devient possible.

Un rôle sans privilège

L'application se connecte avec un rôle ni super-utilisateur ni BYPASSRLS ; le script d'installation de production s'arrête si ce n'est pas le cas.

Contenus sur une origine séparée

Paquets SCORM et contenus HTML déposés sont servis depuis un sous-domaine distinct, hors de portée du cookie de session ; les fichiers, par des liens signés valables cinq minutes.

03 · IDENTITÉ ET ACCÈS

SSO, SCIM, MFA, sessions : ce que votre politique exige.

Connexion unique

SAML 2.0, OpenID Connect, Microsoft Entra ID ou Google, avec création des comptes à la première connexion.

MFA imposable

Code à usage unique (TOTP), imposable aux administrateurs — activé par défaut sur un nouvel espace — ou à tout le personnel. Avec le SSO, la MFA de votre fournisseur d'identité s'applique.

Mots de passe

Hachage Argon2id ; verrouillage de quinze minutes après cinq échecs.

Provisionnement SCIM 2.0

Création, mise à jour et suspension des comptes depuis votre annuaire.

Expiration d'inactivité

Réglable par organisation : 30 minutes par défaut pour les administrateurs, 8 heures pour les autres. Sessions liées à l'appareil et révocables.

Accès du support encadré

En lecture seule, sur votre autorisation, sept jours au plus ; chaque lecture est inscrite à votre journal d'audit.

04 · TRAÇABILITÉ

Un journal en ajout seul, protégé par la base.

Connexions, comptes, rôles, exports, consultations de données individuelles, accès du support : chaque action sensible est inscrite avec son auteur, sa cible et les différences. Un déclencheur PostgreSQL refuse toute modification ou suppression ; seule la purge à la durée de conservation que vous réglez y touche.

- ✓ Auteur, cible, différences
- ✓ Modification refusée par la base
- ✓ Conservation réglable de 1 à 10 ans (2 ans par défaut)

05 · CHIFFREMENT

Chiffré en transit, secrets chiffrés au repos.

 En transit

HTTPS partout, HSTS de deux ans, certificats Let's Encrypt renouvelés automatiquement.

 Sauvegardes chiffrées

Chiffrées par l'outil de sauvegarde (AES-256) avant d'être écrites dans le dépôt.

 Secrets chiffrés

Clés MFA, secrets SSO, clés de signature et jetons d'intégration sont chiffrés dans la base par l'application.

 Liens signés

Aucun fichier en accès public : chaque téléchargement passe par un lien signé qui expire.

06 · CONTINUITÉ

Sauvegardé, restauré, chronométré.

 Restauration à un instant précis

Journal des transactions archivé en continu (pgBackRest), sauvegarde complète le dimanche, différentielle les autres nuits, quatre semaines d'historique.

 15 minutes, 4 heures

Nos objectifs : 15 minutes de données perdues au plus, remise en service en 4 heures. L'exercice est prévu chaque mois en production.

 Un exercice chronométré

Le 10 octobre 2026 : une base de 173 Mo restaurée à un instant précis en une trentaine de secondes, de bout en bout ; 126 086 notes sur 126 086 retrouvées.

 Un second hébergeur

Avant toute donnée réelle, le dépôt de sauvegarde est placé chez un second hébergeur, distinct du premier.

07 · SOUS-TRAITANTS

Qui traite vos données, et quand.

L'IA se désactive par organisation, fonction par fonction ou en entier. Sur une instance au Maroc, données et sauvegardes restent au Maroc ; l'IA et l'envoi d'e-mails sont alors les seuls services hors du Maroc, et chacun peut être désactivé ou remplacé.

SOUS-TRAITANT	RÔLE	LIEU	QUAND
Hetzner Online GmbH	Hébergement : serveurs, base de données, fichiers, sauvegardes.	Allemagne (UE)	Toujours
OpenAI ou Anthropic (un seul)	Fonctions d'IA. Les personnes y sont désignées par des identifiants pseudonymes ; selon les conditions d'API du fournisseur, les données envoyées ne servent pas à entraîner ses modèles.	États-Unis	Si l'IA est activée
Let's Encrypt (ISRG)	Certificats HTTPS. Ne reçoit que les noms de domaine, aucune donnée personnelle.	États-Unis	Toujours
Prestataire d'envoi d'e-mails	Invitations, notifications et rapports programmés par e-mail. Nommé dans l'accord de sous-traitance.	Nommé au contrat	Si l'e-mail est activé

SOUS-TRAITANT	RÔLE	LIEU	QUAND
Meta (WhatsApp Business)	Rappels WhatsApp, aux seules personnes qui les ont acceptés.	Selon Meta	Si vous l'activez

08 · RÉVERSIBILITÉ

Partir avec tout, à tout moment.

Votre administrateur génère une archive complète : chaque table au format NDJSON, les fichiers, chaque cours au format IMS Common Cartridge, un manifeste et un mode d'emploi en trois langues. Lien signé valable 24 heures, téléchargement tracé, archive supprimée après sept jours.

- ✓ Formats ouverts
- ✓ Cours réimportables dans une autre plateforme
- ✓ Sans frais de sortie

09 · ÉVALUATION

Ce que nous avons vérifié, et ce qui reste à faire.

- Une auto-évaluation interne selon l'OWASP ASVS 4.0.3, niveau 2, datée du 10 octobre 2026 : 160 exigences satisfaites, 10 partiellement, 25 sans objet. C'est notre propre revue, pas un audit.
- Un test d'intrusion externe est planifié avant la mise en production avec des données réelles. Son cahier des charges est écrit.
- À chaque livraison : tests d'isolation entre clients, matrice des droits de chaque rôle, analyse statique de sécurité, audit des dépendances et recherche de secrets.
- Nous ne détenons ni certification ISO 27001 ni rapport SOC 2, et ne prétendons pas le contraire.

10 · CADRE LÉGAL

Loi 09-08, loi 05-20 et vos obligations.

- Loi 09-08 : vous êtes responsable du traitement, nous agissons comme sous-traitant, dans un accord de traitement des données.
- Pour votre espace, la plateforme prépare le registre des traitements, un projet de déclaration CNDP, l'accord de sous-traitance, la liste des sous-traitants et les durées de conservation, à faire valider par votre juriste.
- Durées de conservation réglables ; export et anonymisation à la demande — l'anonymisation garde les notes pour vos statistiques.
- Loi 05-20 : si vos obligations imposent un hébergement national, une instance dédiée au Maroc permet d'y répondre, à valider avec votre RSSI.

11 · SECTEUR BANCAIRE

Externalisation dans le secteur bancaire.

Une banque qui confie un service à un prestataire doit pouvoir le localiser, le contrôler et en sortir. Le service peut être hébergé au Maroc, sur une instance qui vous est dédiée. Le contrat prévoit votre droit d'audit et la réversibilité, avec l'export complet décrit plus haut.

- ✓ Hébergement au Maroc possible
- ✓ Droit d'audit prévu au contrat
- ✓ Réversibilité prévue au contrat

Questions de votre RSSI

Le questionnaire de sécurité de votre établissement, une revue d'architecture ou un accès à l'auto-évaluation détaillée : écrivez-nous.

contact@whiteboard.ma

Whiteboard · whiteboard.ma · Version du 15 octobre 2026