FICHE DE CORRECTION / P1C4

Analysez la sécurité des échanges

CulturaLab · Activité « À vous de jouer »

L’essentiel

La configuration B est à recommander : elle réduit les données transmises et limite les risques liés aux clés et au webhook. Ces configurations sont fictives : leur description ne prouve pas que les protections fonctionnent réellement.

1 · Champs à transmettre

À partir des tables Adhérents et Événements, retenez uniquement les informations utiles à l’inscription. Le nom complet se construit à partir de deux champs de la table Adhérents.

Source CulturaLab	Destination billetterie	Décision
Prénom + Nom	Nom complet	Transmettre les deux champs combinés.
E-mail	E-mail	Transmettre.
Événement inscrit / choisi	Événement	Transmettre l’événement concerné par l’inscription.
Téléphone, adresse postale, date de naissance, notes internes	—	Ne pas transmettre : ces champs ne sont pas nécessaires ici.

2 · Les cinq contrôles

Comparez les descriptions des configurations A et B dans l’énoncé. La portée des jetons et le plan de rotation sont des informations du scénario, pas des éléments à rechercher dans la base Airtable.

Comparer et recommander

Contrôle	Configuration A	Configuration B
Stockage de la clé	Fausse clé inscrite en clair dans l'URL.	Clé rangée dans les Credentials n8n.
Portée du jeton Airtable	Tous les droits sur toutes les bases.	Lecture limitée à la base CulturaLab, selon les besoins du scénario.
Webhook	Aucune authentification : une requête non autorisée peut être acceptée.	Un jeton secret est exigé dans l'en-tête.
Mapping	Fiche adhérent complète transmise.	Nom complet, e-mail et événement choisi uniquement.
Rotation	Aucun plan prévu.	Fréquence fixée selon le risque ; révocation immédiate en cas de fuite ou de départ d'une personne ayant accès.

3 · Exemple de note à la présidente

Je recommande la configuration B, sous réserve de vérifier ses réglages avant l'ouverture.
Elle ne transmet à la billetterie que le nom complet, l'e-mail et l'événement concerné.
La clé est rangée dans les Credentials et le jeton Airtable est limité à la lecture de la base CulturaLab.
Le webhook demande un jeton secret et un plan prévoit le renouvellement des clés.
À l'inverse, la configuration A expose une clé dans l'URL, donne des droits trop larges et transmet toute la fiche.
Elle accepte aussi les appels au webhook sans authentification et ne prévoit aucune rotation.
Avant la mise en production, vérifiez les droits réels du jeton, le stockage des secrets et le mapping sur une inscription fictive.
Vérifiez aussi que le webhook refuse une requête non authentifiée et désignez une personne chargée de la rotation.
La configuration B ne doit être retenue qu'après ces vérifications ; la décision finale vous revient.

Erreurs fréquentes

Confondre une clé configurée avec une clé protégée ; transmettre toute la fiche « au cas où » ; oublier le webhook ; présenter une protection décrite dans le scénario comme une preuve de son bon fonctionnement.