

Ce que tu ne branches pas sans cadre

Quatre refus de prudence, puis une question pour décider du reste

Module BR3 - CADRER - 7 min - version 1.1

Brancher un outil peut rendre un usage plus fluide. Cela crée aussi un accès durable qu'il faut pouvoir expliquer, limiter et retirer.

Le module ne classe pas les produits en « sûrs » ou « dangereux ». Il apprend à décider avant d'accorder l'accès.

Ce que tu sauras faire en sortant

- Appliquer quatre refus par défaut propres au parcours Solutio.
- Décrire le dommage plausible et le mécanisme de détection avant d'accorder un autre accès.
- Vérifier le périmètre réel et la révocation dans le produit au lieu de les supposer.

L'essentiel, en trente secondes

Politique de prudence Solutio : quatre cas ne s'accordent pas dans cet exercice sans cadre validé.

- Accès qui peut agir vers l'extérieur sans validation humaine préalable.
- Accès qui peut déclencher ou modifier une opération financière/comptable.
- Accès à un espace contenant des données de personnes ou des informations sensibles qui n'ont pas passé le tri F3 et le cadre approprié.
- Accès dont tu ne sais pas comment réduire le périmètre ou révoquer l'autorisation.

Pour les autres cas, pose une question :

Si cet accès faisait autre chose que ce que j'attends, qu'est-ce qui pourrait être affecté, et comment m'en apercevrais-je ?

Si tu ne sais pas répondre, reporte la connexion le temps de vérifier.

Pourquoi ces quatre refus

Ils ne sont pas présentés comme des lois générales. Ils réduisent quatre risques faciles à comprendre :

- sortie externe : une action peut toucher un tiers avant ta relecture ;
- argent/comptabilité : l'impact dépasse le simple brouillon de texte ;
- données de personnes : un accès permanent n'a pas la même portée qu'un exemple fictif collé ponctuellement ;
- révocation inconnue : tu ne peux pas encore démontrer que l'accès est sous contrôle.

Le bon niveau de précision est le suivant : « je refuse par défaut tant que le cadre n'est pas démontré », pas « ce type d'accès est toujours interdit ».

Deux cas à examiner sans supposer le comportement du produit

Agenda

Un agenda peut révéler des noms, des lieux ou le motif d'un rendez-vous. Avant toute connexion :

- vérifie exactement ce que le produit demande à lire ou modifier ;
- cherche l'option la plus étroite disponible ;
- utilise un calendrier de test si tu peux ;
- observe comment retirer l'accès.

Le module ne suppose pas qu'un accès en lecture rendrait automatiquement tout l'agenda disponible dans toutes les conversations. Cette portée doit être relevée pour le produit concerné.

Messagerie

Une boîte complète contient des contenus de nombreux tiers et des périodes différentes. La politique Solutio est de préférer, lorsqu'il existe et qu'il est réellement respecté par le produit, un périmètre dédié préparé pour l'usage plutôt qu'un accès global.

Là encore : « dossier dédié » est une recommandation de minimisation, pas la preuve que chaque connecteur sait limiter son accès à ce dossier.

Micro-défi

Trois demandes fictives :

- lecture d'un dossier de documentation créé uniquement pour le test ;
- accès à une boîte mail complète ;
- possibilité de créer des événements chez d'autres personnes.

Réponse attendue dans la politique Solutio : commencer par le 1, et reporter 2/3 tant que le besoin, le périmètre, la validation humaine et la révocation ne sont pas documentés.

Le cas où ça se passe mal

Cas reconstitué pour l'exercice.

Tu accordes un accès de lecture à un espace de test. Plus tard, tu déplaces dans ce même espace un document qui n'était pas destiné au connecteur.

Le problème n'est pas un comportement mystérieux du modèle. Tu as changé le contenu du périmètre accordé après la décision initiale.

Correction : un accès se revoit avec son périmètre. La revue porte sur ce qui est autorisé aujourd'hui, pas seulement sur ce qui s'y trouvait au moment du branchement.

Ce que ce module ne règle pas

- Il ne dit pas quelles permissions un produit donné demande réellement.
- Il ne garantit pas qu'un mode « lecture seule » existe ou empêche toute sortie d'information.
- Il ne définit pas tes obligations contractuelles, de confidentialité ou de données.
- Il ne juge pas un éditeur.
- Il ne prouve pas qu'un dossier dédié limite techniquement le connecteur : cela doit être observé.

Quand tu t'arrêtes

- Le produit demande une permission plus large que celle que tu pensais accorder.
- Tu ne sais pas si l'accès est en lecture, en écriture ou mixte.
- Tu ne sais pas retirer l'accès.
- L'espace contient des informations qui n'ont pas passé le tri F3.

- Tu ne peux pas expliquer qui ou quoi serait affecté en cas d'erreur.

À toi

Fais l'exercice sur une connexion fictive ou un espace de test sans données réelles.

- Besoin. Écris en une phrase ce que la connexion doit permettre.
- Périmètre. Liste ce qu'elle doit voir et ce qu'elle ne doit pas voir.
- Impact. Écris ce qui pourrait être affecté si l'accès se comportait autrement que prévu.
- Détection. Écris le signe qui te permettrait de détecter le problème.
- Révocation. Repère réellement comment l'accès se retire avant de considérer l'exercice réussi.

C'est réussi si :

- le besoin tient en une phrase ;
- le périmètre est plus petit que « tout mon compte » ;
- l'impact et le signal de détection sont nommés ;
- la révocation est observée, pas supposée ;
- aucune donnée réelle sensible n'a servi au test.

Vérifie ton geste

- Tu ne sais pas révoquer. Tu reportes la connexion.
- Le périmètre affiché est plus large que ton besoin. Tu cherches une permission plus étroite ou tu renonces.
- L'accès concerne des données de personnes. Tri F3 + cadre applicable avant connexion.
- Le produit annonce "lecture seule". Tu peux limiter le risque d'action, mais tu ne déduis pas de ce libellé ce qui peut ressortir dans une réponse ; tu vérifies la portée réelle.
- Tu as oublié ce qui est connecté. Inventaire et revue maintenant.

Seuil de réussite : 4 sur 5, questions 1 et 2 obligatoires.

Selon ce que tu obtiens

L'accès est plus large que prévu. N'essaie pas de compenser par une instruction textuelle ; réduis techniquement le périmètre ou reporte.

Tu ne trouves pas la révocation. C'est un échec du test, pas une invitation à cliquer quand même.

Le périmètre est limité et révocable. Garde une date de revue : le contenu de l'espace et les permissions peuvent évoluer.

Tu es bloqué. Fais seulement l'inventaire des connexions et permissions déjà actives. Ce constat est déjà une preuve observable.

Fiche mémo

- Les « quatre non » sont une politique Solutio de prudence.
- Besoin précis avant permission.
- Périmètre minimal observé, pas supposé.
- Données sensibles F3 + cadre expert.
- Impact + signal de détection avant connexion.

- Révocation observée + date de revue.

Ce que tu viens de pratiquer

- Tu as remplacé des interdits présentés comme universels par une politique de prudence explicite.
- Tu as documenté besoin, périmètre, impact, détection et révocation.
- Tu sais que le comportement exact d'un connecteur se relève dans le produit concerné.

Sources et statut : docs/bloc-brancher-PROVENANCE.md. BR3 reste S3 et brouillon jusqu'à la revue experte et au test utilisateur requis.