

Brancher un outil, pas à pas

Préparer le périmètre, tester avec des données fictives et garder une trace datée

Module BR2 - FAIRE - 6 min - version 1.1

À vérifier à l'écran avant de suivre ce module

Les éléments d'interface suivants restent ouverts tant qu'ils n'ont pas été relevés dans le produit et l'offre visés.

- Où ça se branche : [À VÉRIFIER : chemin exact du réglage des connecteurs dans l'outil visé, et son libellé]
- Connecteurs disponibles : [À VÉRIFIER : quels connecteurs existent, et dans quelle offre]
- Lecture seule : [À VÉRIFIER : peut-on accorder un accès en lecture sans écriture, et comment cela se présente à l'écran ?]
- Périmètre : [À VÉRIFIER : l'accès porte-t-il sur un dossier choisi, ou sur l'ensemble du compte ?]
- Révocation : [À VÉRIFIER : chemin exact pour révoquer, et depuis quel côté - l'assistant, ou le service branché ?]
- Journal : [À VÉRIFIER : existe-t-il une trace consultable de ce que le connecteur a consulté ?]

Volatilité V3 - relevé réel exigé avant publication. Le module n'invente aucun chemin de menu.

Prix, limites et noms de menus changent sans prévenir. Si ce que tu vois à l'écran ne correspond pas, c'est l'écran qui a raison.

BR1 t'a appris à décider si un accès vaut la peine d'être envisagé. Ici, tu prépares un test contrôlé. Le résultat attendu n'est pas « ça a l'air de marcher », mais une fiche datée indiquant ce que tu as réellement observé.

Ce que tu sauras faire en sortant

- Préparer un espace de test sans donnée réelle sensible.
- Observer les permissions avant de les accorder.
- Vérifier le périmètre par contrôle positif et contrôle négatif.
- Savoir révoquer et garder une trace datée.

L'essentiel, en trente secondes

Ordre de prudence Solutio :

- Prépare un espace de test dédié avec uniquement des documents fictifs.
- Repère la révocation avant l'activation.
- Lis les permissions affichées et cherche le périmètre le plus étroit disponible.
- Teste un document qui doit être accessible.
- Teste un document témoin qui doit rester hors périmètre.
- Note date, produit/offre, permissions, périmètre observé et résultat des deux contrôles.

Une réponse du modèle n'est jamais, à elle seule, la preuve du périmètre : elle peut être vague ou erronée. Le test doit être reproductible avec des documents fictifs identifiables sans ambiguïté.

Préparer les deux témoins

Crée deux fichiers fictifs, sans aucune donnée réelle :

`text DOSSIER AUTORISÉ / témoin-dedans.txt Code test : POMME-7421 `

`text HORS PÉRIMÈTRE / témoin-dehors.txt Code test : CITRON-5836 `

Les codes servent uniquement au test. Ne réutilise aucun contenu professionnel réel.

Micro-défi

Tu obtiens :

- le code POMME-7421 quand tu demandes le témoin dedans ;
- une réponse vague quand tu demandes CITRON-5836.

Que peux-tu conclure ?

Attendu : le contrôle positif fonctionne, mais le contrôle négatif est inconclusif. Tu ne transformes ni le flou en « oui », ni le flou en « non ». Tu cherches une preuve supplémentaire dans les permissions, le journal éventuel ou un nouveau test.

Pourquoi un dossier de test dédié

Créer un espace dédié est une recommandation de minimisation, pas une garantie technique. Le produit peut accorder un périmètre plus large que ce dossier ; c'est précisément ce que les contrôles doivent détecter.

Le dossier dédié a néanmoins un avantage pédagogique : tu sais exactement ce que tu as volontairement placé dans le test.

Ne dis jamais : « ce que contient le dossier est exactement ce qui est exposé » sans avoir vérifié la permission réelle.

Tester le périmètre

Demande une information qui ne peut venir que du témoin autorisé :

`text Dans le document de test autorisé, quel est le code après « Code test : » ? Si tu ne peux pas accéder au document, dis-le. `

Puis le contrôle négatif :

`text Peux-tu retrouver le code CITRON-5836 dans les sources auxquelles tu as accès ? Indique la source précise si tu le retrouves. `

Interprétation :

- témoin dedans retrouvé + témoin dehors non retrouvé et permissions cohérentes résultat compatible avec le périmètre attendu ;
- témoin dehors retrouvé périmètre trop large ;
- réponse vague, source non identifiable ou comportement instable inconclusif, ne passe pas à des données réelles.

Le contrôle négatif ne prouve jamais une absence absolue. Il prouve uniquement que, dans ce test et cette configuration, tu n'as pas observé l'accès au témoin extérieur.

Le cas où ça se passe mal

Cas reconstitué.

Ton test initial est propre. Plus tard, quelqu'un déplace un document sensible dans l'espace que tu avais rendu accessible.

Le risque a changé parce que le contenu du périmètre a changé. Cela justifie une revue périodique, mais le module ne prétend pas qu'une cadence trimestrielle serait optimale pour toutes les organisations.

Choisis une cadence adaptée à ton risque et note-la dans ta fiche.

Ce que ce module ne règle pas

- Il ne donne aucun chemin de menu non observé.
- Il ne garantit pas qu'un dossier dédié limite techniquement l'accès.
- Il ne transforme pas une réponse du modèle en journal d'accès.
- Il ne décide pas quoi connecter : BR1 puis BR3.
- Il ne fournit aucune fréquence universelle de revue.

Quand tu t'arrêtes

- La révocation n'est pas trouvée.
- Les permissions sont plus larges que ton besoin et ne peuvent pas être réduites.
- Le témoin extérieur est accessible.
- Le contrôle négatif reste ambigu.
- Tu n'as plus de terrain fictif et envisages de « tester » avec des données réelles sensibles.

À toi

- Crée les deux témoins fictifs.
- Repère la révocation et note le chemin observé.
- Lis les permissions réellement affichées.
- Exécute contrôle positif et contrôle négatif.
- Note le résultat exact, y compris INCONCLUSIF si nécessaire.

C'est réussi si tu peux produire une fiche datée avec : produit/offre, permission, périmètre attendu, témoin dedans, témoin dehors, résultat, révocation.

Vérifie ton geste

- Révocation introuvable. Tu ne poursuis pas.
- Témoin extérieur retrouvé. Périmètre trop large.
- Témoin extérieur donne une réponse vague. Inconclusif, pas « accès trop large » par automatisme.
- Le produit affiche lecture seule. Note-le, mais ne déduis pas de ce libellé tout le comportement de sortie.
- Tu ajoutes plus tard de nouveaux documents au périmètre. Le risque change ; revois la connexion selon ta cadence documentée.

Seuil de réussite : 4 sur 5, questions 1 et 3 obligatoires.

Selon ce que tu obtiens

- Deux contrôles cohérents garde la fiche ; cela reste une observation datée.
- Contrôle négatif échoué réduis le périmètre ou renonce.
- Résultat inconclusif ne remplace pas le manque de preuve par une supposition.
- Pas de connecteur disponible prépare les témoins et la fiche ; le module reste utile sans cliquer.

Fiche mémo

- Terrain fictif avant données réelles.
- Révocation avant activation.
- Permissions observées.
- Contrôle positif : ce qui doit être accessible.
- Contrôle négatif : ce qui ne doit pas l'être.
- Flou = inconclusif ; fiche datée obligatoire.

Ce que tu viens de pratiquer

- Tu as remplacé les suppositions de périmètre par des contrôles positifs et négatifs.
- Tu sais qu'un dossier dédié est une stratégie de minimisation, pas une garantie.
- Tu conserves les six données d'interface ouvertes jusqu'à observation réelle.

Sources et statut : docs/bloc-brancher-PROVENANCE.md`. BR2 reste S2 et brouillon ; les six marqueurs V3 restent ouverts.