OPTI'

Dossier sécurité et protection des données

Comment Opti' protège les comptes, les documents et les données de collecte de ses utilisateurs, et ce que chaque organisation doit savoir avant de lui confier les siennes.

BROUILLON · à relire par l'éditeur avant toute diffusion

Version	0.9, brouillon du 16 novembre 2026
Éditeur	LEQUEUX Thomas Consulting, éditeur d'Opti'
Destinataires	responsables de la sécurité, de la protection des données et des achats des organisations clientes
Contact sécurité	consulting@lequeux-thomas.com, objet « Sécurité »
Version en ligne	myoptibot.com/securite/

Sommaire

1 Lire ce document
2 Architecture et hébergement
3 Les données et leur protection
4 Comptes et connexion
5 Qui accède à quoi
6 Collecte de données sur le terrain
7 Chiffrement et clés
8 Stockage dans l'espace de l'organisation
9 Intelligence artificielle
10 Sous-traitants
11 Protection des données personnelles
12 Sauvegardes et continuité
13 Développement et correctifs
14 Journaux et incidents
15 L'exploitation du service
16 Limites à connaître
17 Documents complémentaires
A Annexe : conformité OWASP ASVS
B Annexe : OWASP Top 10 de l'IA

1 Lire ce document

Opti' est une plateforme de suivi, d'évaluation, de redevabilité et d'apprentissage (MEAL) pour le secteur humanitaire : un assistant spécialisé (OptiBot), un espace de gestion de projet et de collecte de données (Opti Gemba), un coach de formation (Opti Academy). Elle est disponible en application web (myoptibot.com/app, installable sur ordinateur et téléphone, Android compris) et en complément pour Microsoft Excel.

Ce dossier décrit ce qui est **en place** à sa date, pas ce qui est prévu. Les limites connues sont rassemblées en section 16.

Le cadre de travail

- **Référentiel de sécurité applicative** : OWASP ASVS 5.0.0 (mai 2025), niveaux 1 et 2, évalué exigence par exigence en interne ; pour les fonctions d'IA, le Top 10 OWASP des applications à base de modèles de langage (2025).
- **Protection des données** : règlement général sur la protection des données (RGPD) ; Opti' est édité en France.
- **Évaluation** : audit interne mené en novembre 2026. Opti' n'est pas certifié ISO 27001 ni SOC 2, et aucun test d'intrusion externe n'a encore été conduit.

Les principes qui reviennent dans tout le dossier

Principe	Ce qu'il veut dire chez Opti'
Hébergement dans l'Union européenne	base de données en Suède, serveur d'application en Allemagne, fichiers de l'application en France.
Chiffrement en plus de celui des hébergeurs	les données les plus sensibles (réponses de collecte, conversations, jetons d'accès) sont chiffrées par Opti' avant d'être écrites.
Contrôle d'accès dans la base elle-même	chaque table porte ses règles ; une table sans règle est fermée par défaut.
Travail hors connexion	la saisie de terrain continue sans réseau, et se synchronise au retour de la connexion.
Aucun entraînement sur les données	ni par Opti', ni par les fournisseurs de modèles utilisés.
Le client peut garder ses documents chez lui	Google Drive ou SharePoint, avec un accès limité à ce qu'Opti' y crée ou à un seul site.

2 Architecture et hébergement

Opti' se compose de quatre éléments : l'application, qui s'exécute dans le navigateur de l'utilisateur ; une API, qui porte tout ce qui demande un secret (chiffrement, IA, paiement, envoi d'e-mails) ; une base de données avec son service d'authentification ; et des fournisseurs spécialisés, appelés uniquement par l'API.

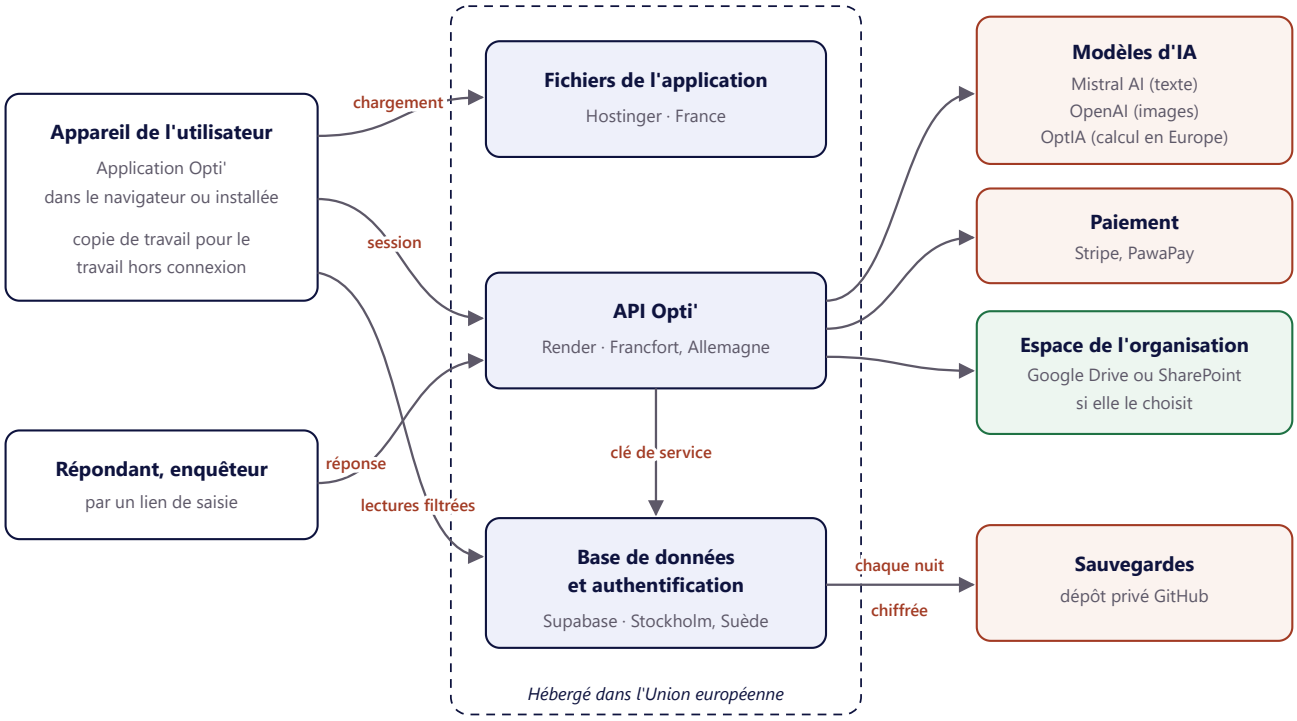


Figure 1. Les composants d'Opti' et leurs échanges. Tous passent en HTTPS. Les fournisseurs à droite ne sont appelés que par l'API, jamais par le navigateur.

Deux chemins vers la base, un seul contrôle

L'application lit et écrit une partie des données directement dans la base, avec le jeton de session de la personne connectée : la base applique alors ses propres règles d'accès, ligne par ligne. Tout ce qui demande un secret passe par l'API, qui vérifie le jeton, impose l'identité qu'il porte (jamais celle qu'annoncerait le navigateur), puis agit avec la clé de service.

Où sont les serveurs

Composant	Fournisseur	Lieu
Base de données, authentification, factures	Supabase	Stockholm, Suède (relevé dans la console)
API	Render	Francfort, Allemagne (relevé)
Fichiers de l'application et des sites, e-mails du service	Hostinger	France ; sauvegardes de l'hébergeur en Lituanie
OptIA, le modèle d'IA privé d'Opti'	Modal (location de processeurs graphiques)	calcul aux Pays-Bas (mesuré) ; point d'entrée des requêtes aux États-Unis
Sauvegardes chiffrées	GitHub	non garanti ; les fichiers sont chiffrés avant de partir (section 12)

Les protections du navigateur

- HTTPS seulement, avec HSTS : le navigateur refuse toute connexion non chiffrée.
- Une politique de sécurité du contenu n'autorise que les scripts attendus, désignés par leur empreinte ; les violations sont remontées au serveur.
- L'application ne peut pas être affichée dans le cadre d'un autre site.
- L'API n'accepte que les origines d'Opti' et applique des plafonds de requêtes par compte et par adresse réseau.

3 Les données et leur protection

Opti' range ses données en trois niveaux. Le niveau décide de la protection.

Niveau	Données	Protection
Confidentiel	réponses de collecte et photos ; conversations avec OptiBot et son profil de l'utilisateur ; rapports enregistrés ; analyses ; focus groups ; jetons d'accès aux comptes tiers (KoboToolbox, Google, Microsoft)	chiffrées par l'API avant écriture (AES-256-GCM), en plus du chiffrement de l'hébergeur ; jamais écrites dans un journal
Personnel	adresse e-mail, nom, formule, projets, questionnaires, termes de référence, factures, journal de connexion	accès limité au titulaire et aux personnes qu'il invite, par les règles de la base ; chiffrement de l'hébergeur
Public	tarifs, contenu des sites, chiffres agrégés	intégrité seulement

Où vit chaque donnée

Donnée	Où	Chiffrée par Opti'	Qui la lit
Compte : adresse, mot de passe, second facteur	authentification Supabase	mot de passe haché (bcrypt)	le titulaire
Projets et documents d'Opti Gemba	base ; copie sur l'appareil	non	le titulaire et les membres du projet, selon leur rôle
Réponses de collecte	base	**oui**	les membres de la collecte, par l'API ; un enquêteur connecté, ses propres réponses
Conversations OptiBot, rapports enregistrés	base	**oui**	le titulaire, par l'API
Bibliothèque de documents d'OptiBot	base, tables fermées au navigateur	non	l'API, pour le titulaire et ceux avec qui il partage
Jetons KoboToolbox, Google, Microsoft	base	**oui**	l'API seule ; jamais renvoyés au navigateur
Données de carte bancaire	Stripe uniquement	sans objet	jamais visibles par Opti'
Sauvegardes	dépôt privé	**oui**, avant de partir	l'éditeur, avec une clé gardée hors ligne

Ce qui reste sur l'appareil

Pour travailler sans réseau, l'application garde sur l'appareil une copie des documents ouverts, les réponses pas encore envoyées et, selon le choix de la personne, des conversations privées. **À la déconnexion**, tout ce qui a une copie en ligne est effacé de l'appareil. Ce qui n'existe encore que là (une réponse saisie sans réseau, une conversation enregistrée localement) est d'abord montré à la personne, qui peut l'envoyer, le garder, ou le supprimer définitivement : rien n'est perdu sans qu'elle l'ait décidé.

4 Comptes et connexion

Les voies de connexion

Voie	Contrôle
Adresse e-mail et mot de passe	au moins 8 caractères ; aucune règle de composition ni renouvellement forcé (recommandation NIST SP 800-63B) ; gestionnaires de mots de passe et collage permis ; mot de passe haché par bcrypt
Code ou lien reçu par e-mail	à usage unique, valable 10 minutes
Microsoft	OpenID Connect ; un compte Opti' existant est relié, jamais dupliqué
Google	OpenID Connect, même règle
LinkedIn	OpenID Connect

L'adresse e-mail est confirmée avant la première connexion. Aucune question secrète, aucun compte par défaut.

La double authentification

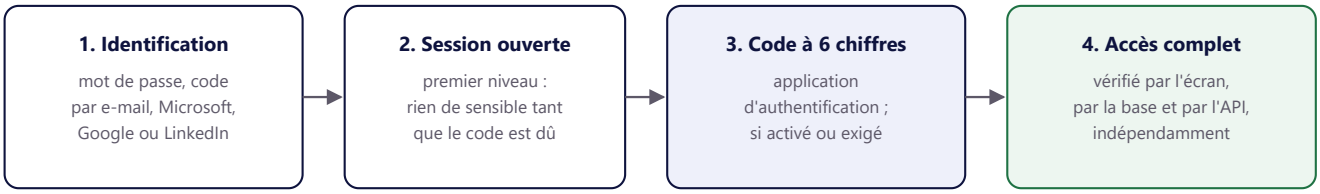


Figure 2. La connexion. Le second facteur n'est pas une simple étape d'écran : la base et l'API refusent d'elles-mêmes une session qui ne l'a pas passé quand il est dû.

- Gratuite, activable par chacun depuis Mon compte, onglet Sécurité.
- **Exigible par une organisation** : le propriétaire d'une équipe, ou un administrateur qu'il a nommé, peut l'imposer à tous les membres, depuis l'onglet Équipe.
- Hors connexion, rien n'est bloqué ; le code est demandé au retour du réseau.
- Un facteur perdu n'est retiré qu'après une demande écrite depuis l'adresse du compte.

Défense contre les essais en masse

Les points de connexion limitent le débit par adresse réseau : 30 connexions ou vérifications de code par tranche de 5 minutes. Avec un code à 6 chiffres valable 10 minutes, cela laisse au plus 60 essais par code sur un million de combinaisons. Opti' ne bloque pas un compte après des échecs : ce blocage permettrait à un tiers de fermer le compte de quelqu'un d'autre.

Les sessions

Jeton d'accès	valable une heure, renouvelé automatiquement
Jeton de renouvellement	remplacé à chaque usage ; refusé par le serveur après la déconnexion
Changement de mot de passe	propose de fermer toutes les autres sessions du compte
Durée maximale d'une session	aucune : une session qui expirerait hors connexion empêcherait la saisie sur le terrain. La double authentification et la fermeture des autres sessions portent ce risque

5 Qui accède à quoi

Les règles d'accès vivent **dans la base de données et dans l'API**, jamais seulement dans l'écran. Toutes les tables portent des règles d'accès par ligne ; une table sans règle est fermée au navigateur par défaut. Les fonctions de la base ouvertes aux comptes connectés lisent l'identité de l'appelant et n'acceptent pas qu'on leur en désigne une autre.

Rôle	Ce qu'il peut faire
Titulaire du compte	tout sur ses propres données
Membre lecteur d'un projet	lire le projet auquel il a été invité, après avoir accepté l'invitation
Membre éditeur d'un projet	modifier le projet, si la formule de l'organisation autorise le travail à plusieurs ; sinon, il est traité en lecteur
Propriétaire ou administrateur d'équipe	inviter et retirer des membres, attribuer des sièges, exiger la double authentification ; pas de lecture des documents personnels des membres
Répondant par lien	lire le questionnaire seul et **ajouter** une réponse ; un enquêteur connecté retrouve ses propres réponses, jamais celles des autres
Visiteur sans compte	aucune donnée d'un compte

L'éditeur d'Opti'. Une seule personne administre le service. Son poste de pilotage est protégé côté serveur (session vérifiée et compte inscrit dans une liste fermée) ; il affiche des indicateurs d'exploitation, et ne déchiffre aucun contenu confidentiel. Les contenus chiffrés ne sont lisibles que par l'API, pour le compte qui y a droit.

Liens de partage d'une collecte

Un lien de saisie porte un jeton aléatoire, que seul son auteur peut lire dans l'application. Il donne accès au questionnaire, pas au reste du projet, et ne permet que d'ajouter une réponse à la collecte à laquelle il est rattaché. Un lien se retire à tout moment.

6 Collecte de données sur le terrain

La collecte est le cœur du service et souvent la donnée la plus sensible : des réponses de bénéficiaires de programmes humanitaires, parfois avec photos ou position.



Figure 3. Le chemin d'une réponse. Elle n'est jamais écrite en clair dans la base.

- Une réponse envoyée avec un identifiant qui appartient à une autre collecte est refusée et journalisée.
- Les champs que le serveur impose (collecte, auteur, horodatage) ne peuvent pas être fixés par l'appareil.
- Les photos voyagent dans la réponse et sont chiffrées avec elle.
- L'import depuis KoboToolbox passe par l'API ; le jeton Kobo de l'utilisateur est chiffré, n'est jamais renvoyé au navigateur, et rien ne le journalise.
- Les réponses s'exportent à tout moment (Excel), par les membres autorisés.

7 Chiffrement et clés

Où	Comment
En transit	HTTPS partout, HSTS ; entre l'API et ses fournisseurs aussi
Au repos, chez les hébergeurs	chiffrement des disques par l'hébergeur (AES-256 chez Supabase, documenté)
Au repos, par Opti'	AES-256-GCM (chiffrement authentifié : une donnée altérée est refusée) pour les données confidentielles de la section 3
Mots de passe	hachés par bcrypt, jamais stockés ni journalisés en clair
Sauvegardes	AES-256 avec une clé tirée au hasard chaque nuit, elle-même chiffrée par RSA ; fichier signé (HMAC-SHA256)

La gestion des clés

- La clé de chiffrement des données vit dans le serveur d'application, **pas dans la base** : une copie de la base seule ne permet pas de lire les contenus chiffrés.
- Elle est séquestrée hors ligne, en deux exemplaires rangés en des lieux distincts : sans elle, une sauvegarde serait illisible.
- Elle se renouvelle par versions : une nouvelle version chiffre les écritures nouvelles, l'ancienne reste pour relire l'existant.
- Les clés des fournisseurs ont la portée la plus étroite permise (clé de paiement restreinte, par exemple) et ne quittent pas le serveur.

Qui détient la clé. Les clés sont gérées par Opti', comme dans la plupart des services en ligne : le serveur déchiffre une donnée le temps de la traiter, pour le compte qui y a droit. Une organisation qui veut garder ses documents sous sa propre maîtrise peut les ranger dans son propre espace (section 8).

8 Stockage dans l'espace de l'organisation

Une organisation peut choisir de ranger ses documents dans son propre Google Drive ou dans un site SharePoint. Opti' y écrit avec l'autorisation qu'elle donne, et qu'elle peut retirer à tout moment.

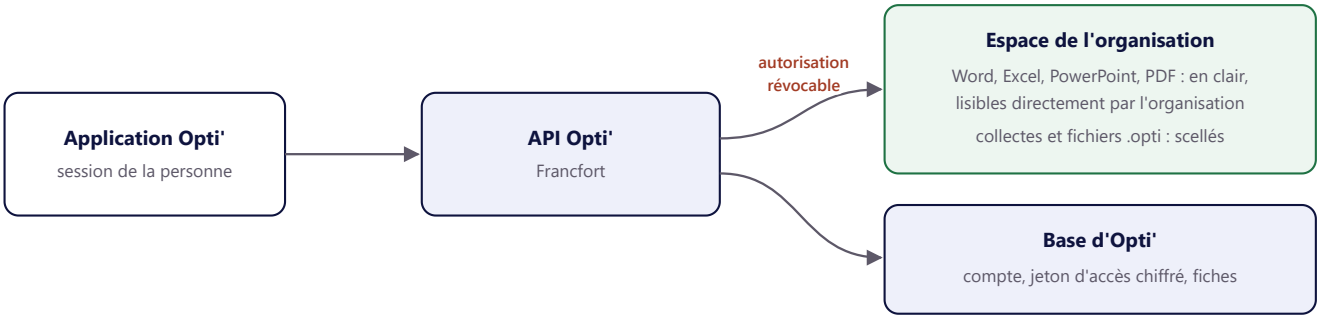


Figure 4. Les documents vont chez l'organisation ; Opti' ne garde que le compte, le jeton d'accès (chiffré) et des fiches techniques.

Fournisseur	Accès demandé par Opti'
Google Drive	`drive.file` : seulement les fichiers qu'Opti' a créés ou que la personne lui a ouverts, jamais le reste du Drive
SharePoint	`Sites.Selected` : **un seul site**, que l'administrateur de l'organisation accorde lui-même, en lecture et écriture ou en contrôle total. Opti' ne voit aucun autre site, ni les espaces OneDrive des personnes. Une notice pas à pas est publiée pour l'administrateur (myoptibot.com/sharepoint-administrateur/)

- Deux écritures concurrentes ne s'écrasent pas : la seconde produit une copie datée à côté.
- Les documents rangés chez l'organisation relèvent de ses propres sauvegardes et de sa propre politique de conservation.

9 Intelligence artificielle

Les modèles sont toujours appelés **par le serveur d'Opti'**, jamais par le navigateur : les clés d'accès ne quittent pas le serveur.

Fonction	Modèle
OptiBot, questionnaires, termes de référence, analyses, rapports, « Demande à tes données »	Mistral Large (Mistral AI, France)
Recherche dans les documents, transcription des focus groups	modèles de Mistral AI
Génération d'images	OpenAI
Recherche web d'OptiBot	moteur Brave Search (pas de modèle)
OptIA, l'IA privée des formules qui l'incluent	Qwen 2.5 72B, exécuté par Opti' sur une machine louée : aucun fournisseur de modèle ne reçoit la demande
Complément Excel, moteur local	modèle exécuté sur l'ordinateur de l'utilisateur : rien ne part

Ce qui part vers le modèle

- Le texte de la demande et l'historique utile de la conversation.
- Les extraits retrouvés **dans la bibliothèque du compte** ou de ce qui lui est partagé ; la recherche reçoit la liste explicite des documents autorisés, et une liste vide l'arrête.
- Pour « Demande à tes données » : les intitulés des questions et des résultats **calculés dans le navigateur** (effectifs, pourcentages, croisements) ; pour certaines opérations, des lignes de données.
- Jamais : les clés, mots de passe et jetons, ni les documents d'un autre compte.

Conservation et entraînement

Fournisseur	Entraînement	Conservation
Mistral AI	désactivé (offre à l'usage)	selon les conditions de Mistral
OpenAI	aucun sur les données de l'API	journaux de surveillance jusqu'à 30 jours
Brave Search	sans objet	requêtes 90 jours au plus
OptIA	aucun : modèle figé, version vérifiée par son empreinte	rien n'est transmis à un fournisseur de modèle
Opti'	aucun entraînement ni affinage	conversations chiffrées, accessibles au seul compte

Garde-fous

Évalués contre le Top 10 OWASP des applications à base de modèles de langage (2025) : détail en annexe B.

- **Le modèle n'agit pas** : ses outils sont tous en lecture. Il ne peut ni écrire, ni envoyer, ni payer, ni supprimer ; toute génération est déclenchée et relue par l'utilisateur.
- **Pas de fuite par un texte piégé** : le modèle ne lit une adresse web que si l'utilisateur l'a donnée ou si la recherche l'a rendue ; les adresses privées sont refusées ; ses réponses n'affichent pas d'images distantes.
- **Affichage sûr** : le texte du modèle est échappé ; le code qu'il écrit pour un calcul s'exécute dans un bac à sable sans réseau ni fichiers.

- **Chiffres contrôlés** : dans un rapport, les chiffres sont calculés sur les données puis rapprochés automatiquement du texte ; les sources sont citées.
- **Méthode publique** : la méthode du générateur de questionnaires et celle du rapport sont publiées, avec une fiche de transparence SAFE AI.

Règlement européen sur l'IA

Lecture de l'éditeur, qui ne vaut pas avis juridique : Opti' intègre des modèles d'usage général dans son propre système, dont l'éditeur est fournisseur ; l'organisation qui l'utilise en est déployeur. Ses usages (questionnaires, analyse de données de suivi, rapports, formation) ne figurent pas parmi les usages à haut risque de l'annexe III. Une organisation qui l'emploierait pour une décision listée par cette annexe, l'accès à une aide par exemple, doit le signaler : l'analyse changerait.

10 Sous-traitants

La colonne « Données » dit ce que le code envoie à chaque fournisseur. Un fournisseur entre dans cette liste **avant** que le code ne lui envoie quoi que ce soit.

Fournisseur	Rôle	Données	Lieu
Supabase	base, authentification, factures	toutes les données du service ; contenus confidentiels chiffrés par Opti'	Suède
Render	serveur d'application	données en transit ; journaux techniques	Allemagne
Cloudflare	réseau devant le serveur, choisi par Render	requêtes chiffrées en transit	réseau mondial
Hostinger	fichiers de l'application et des sites, e-mails du service	aucune donnée d'utilisateur dans les fichiers ; contenu et destinataires des e-mails	France
GitHub	code, sauvegardes	sauvegardes chiffrées avant envoi	non garanti
Mistral AI	IA (texte, recherche, transcription)	demandes et extraits utiles	Union européenne par défaut
OpenAI	images	la description demandée	États-Unis
Modal	machine qui exécute OptIA	demandes adressées à OptIA	calcul aux Pays-Bas ; entrée aux États-Unis
Brave	recherche web	la requête de recherche	non garanti
Google (Firebase)	notifications	jeton de l'appareil, texte de la notification (sans contenu d'utilisateur)	non garanti
Stripe	paiement par carte, factures	adresse, montant, formule ; jamais la carte chez Opti'	non garanti
PawaPay	paiement mobile money	numéro, opérateur, montant ; chaque paiement revérifié avant d'être crédité	non garanti

Services utilisés **à l'initiative de l'utilisateur** : connexion par Microsoft, Google ou LinkedIn ; stockage dans Google Drive ou SharePoint ; import depuis KoboToolbox (serveur choisi par l'utilisateur).

« Non garanti » : le fournisseur ne s'engage pas sur un lieu de traitement dans l'offre utilisée. Plusieurs fournisseurs sont des sociétés américaines, même quand le traitement a lieu en Europe ; voir la section 11 sur les transferts.

11 Protection des données personnelles

Deux rôles

Données	Rôle d'Opti'
Comptes, connexion, abonnements, factures, e-mails du service, journaux	**responsable de traitement**
Questionnaires, réponses de collecte, documents de projet, conversations et rapports d'une organisation cliente	**sous-traitant** : l'organisation décide des finalités, Opti' agit sur ses instructions, sous un accord de traitement (article 28)

Les personnes interrogées dans une collecte, souvent des bénéficiaires de programmes humanitaires, sont des personnes concernées dont Opti' traite les réponses pour le compte de l'organisation. Si un questionnaire porte sur des données de l'article 9 (santé, origine…), la base légale et, le cas échéant, l'analyse d'impact reviennent à l'organisation ; ce dossier lui en fournit la partie technique.

Durées de conservation, appliquées par des tâches automatiques

Donnée	Durée
Journal de connexion, traces de paiement, journal des crédits	13 mois, purge chaque nuit
Mesure d'audience du site et statistiques d'usage de l'IA	13 mois
Corbeille des documents	30 jours
Travaux en cours de l'assistant	7 jours
Réponses de collecte d'un compte repassé à l'offre gratuite	supprimées 15 jours après, après deux e-mails d'avertissement
Documents, collectes, conversations	tant que l'utilisateur ne les supprime pas
Sauvegardes	14 jours (quotidiennes) et 6 mois (mensuelles)
Factures	durée légale de conservation comptable

Les droits des personnes

Accès et portabilité	dans l'application : conversations (Markdown, PDF), réponses (Excel), documents (Word, Excel, PowerPoint, PDF)
Rectification	dans l'application ; sur demande pour le reste
Effacement	chaque document ou conversation dans l'application ; **le compte entier en libre-service** (Mon compte, Gestion du compte), avec double confirmation et code de double authentification s'il est activé ; les factures sont gardées pour l'obligation comptable, et l'opposition aux e-mails commerciaux pour être respectée
Opposition	désabonnement en un clic dans chaque e-mail commercial ; refus de la mesure d'audience ; notifications désactivables

Transferts hors de l'Union européenne

Les données sont hébergées dans l'Union européenne. Certains traitements ont lieu aux États-Unis : génération d'images, transit des demandes à OptIA, recherche web, notifications. Le fondement de chaque transfert (cadre de protection des données UE-États-Unis ou clauses contractuelles types) est en cours de relevé fournisseur par fournisseur ; la liste détaillée des sous-traitants (section 17) le précisera.

12 Sauvegardes et continuité

Quoi	la base entière : structure, données, comptes d'authentification
Quand	chaque jour, par une tâche automatique, avec deux créneaux de rattrapage ; une journée sans sauvegarde déclenche une alerte
Contrôles	un export anormalement petit, ou sans la table des comptes, est refusé plutôt que gardé
Protection	chiffrée **avant de quitter la machine** qui la produit, puis signée ; une altération est détectée avant tout déchiffrement. La clé qui permet de la lire n'est pas chez l'hébergeur des sauvegardes
Conservation	14 sauvegardes quotidiennes et 6 mensuelles
Restauration	essayée et datée : reconstruction complète, contrôle d'empreinte, comptages identiques à la production ; fichier altéré refusé. Un essai est refait au moins chaque trimestre

Si un fournisseur s'arrête

Indisponible	Ce qui s'arrête	Ce qui continue
Base de données	connexion, synchronisation, partage	travail hors connexion sur l'appareil
Serveur d'application	IA, paiement, e-mails, imports	consultation et saisie sur l'appareil
Hébergeur des fichiers	première ouverture sur un nouvel appareil, sites	l'application déjà installée s'ouvre
Fournisseur d'IA	les fonctions d'IA	tout le reste

Une coupure n'efface pas le travail de terrain en cours : il reste sur l'appareil et part au retour du service.

Si l'éditeur est indisponible

Le service fonctionne sans intervention au jour le jour. Une procédure d'accès d'urgence permet à une personne de confiance désignée de maintenir le service, d'arrêter les prélèvements, de garder les noms de domaine et de permettre à chaque organisation de récupérer ses données ; elle ne peut rien supprimer. Chaque compte peut exporter ses données lui-même depuis l'application, à tout moment.

13 Développement, contrôles et correctifs

Référentiel : chaque exigence des niveaux 1 et 2 de l'OWASP ASVS 5.0.0 est évaluée, avec sa preuve (lecture du code, mesure, essai). Le détail, exigence par exigence, est en annexe.

Les contrôles automatiques, à chaque modification

Chaque modification du code passe par une série de contrôles automatiques avant de pouvoir être mise en ligne, puis par la validation de l'éditeur.

Contrôle	Ce qu'il vérifie
Vérification des types	lancée automatiquement après chaque modification de l'application ; une erreur bloque la modification
53 suites d'essais de l'application	logique métier, calculs, stockage local et déconnexion, double authentification, partages, stockage chez l'organisation…
75 suites d'essais du serveur	génération des questionnaires, facturation, paiements, e-mails, notifications, bac à sable du code, contrôles d'identité…
32 fichiers d'essais de la base de données	les règles d'accès : ce que chaque rôle peut lire ou écrire, et surtout ce qu'il ne peut pas
Registre du stockage local	toute donnée gardée dans le navigateur doit être déclarée et classée ; une donnée non déclarée fait échouer les essais
Contrôle des secrets	tout enregistrement du code qui contiendrait une clé, un mot de passe ou une liste d'adresses est refusé
Audit des sites	la publication des sites est refusée en cas d'anomalie bloquante

- **Un essai par défaut corrigé** : un défaut se ferme sur une preuve, l'essai qui le montrait échoue sur la version en ligne. Les essais de sécurité sont eux-mêmes vérifiés : on retire volontairement la protection, l'essai doit échouer.
- **Supervision de l'éditeur** : aucune mise en ligne ni modification de la base de production sans sa décision ; la base ne change que par des migrations versionnées et relues.
- **Pas de préproduction séparée** : base locale et bancs d'essai avant toute mise en ligne, et une copie d'épreuve de l'application pour les nouvelles versions.

Dépendances et délais de correction

Les bibliothèques utilisées sont inventoriées (nomenclature logicielle au format CycloneDX) et surveillées en continu par des alertes automatiques. Une faille dans une dépendance, quand elle touche une partie qu'Opti' utilise, est corrigée dans ces délais, à compter de la publication du correctif :

Faille	Délai
activement exploitée (catalogue de la CISA)	14 jours
critique ou élevée	1 mois
moyenne ou faible	3 mois

Signaler une faille

Une politique de divulgation est publiée (myoptibot.com/securite/, et le fichier standard `security.txt` des deux domaines) : écrire à l'adresse de contact avec « Sécurité » en objet. Accusé de réception sous cinq jours ouvrés,

point d'étape sous trente jours. Une recherche menée de bonne foi dans les limites publiées ne donne lieu à aucune poursuite.

Les e-mails au nom d'Opti'

Le domaine d'où partent les e-mails du service publie ses règles d'authentification (SPF, DKIM, DMARC) ; le domaine de l'application, qui n'envoie aucun e-mail, le déclare et demande le rejet de tout message qui s'en réclamerait.

14 Journaux et incidents

Ce qui est journalisé

Une ligne par requête (heure, identifiant de requête, compte, chemin, statut, durée), les refus d'accès et d'identité, les échecs de second facteur, les refus d'administration, les signatures de paiement invalides, les dépassements de plafonds. **Jamais** : un contenu de collecte, de conversation ou de document, un mot de passe, un jeton ou une clé. Les valeurs journalisées sont neutralisées contre l'injection de lignes. Les journaux ne sont lus que par l'éditeur, et s'effacent au terme fixé par chaque hébergeur.

Réponse à un incident

Six étapes écrites : recevoir et noter, qualifier, contenir (de préférence par un geste réversible), notifier, corriger avec une preuve, tirer les leçons sous deux semaines. Des fiches réflexes couvrent la fuite d'une clé, la compromission du compte d'administration, l'accès non autorisé à des données et l'indisponibilité.

Étape	Délai
Qualification d'un soupçon de violation	24 heures, jours ouvrés
Information de l'organisation cliente dont les données sont touchées	sans retard injustifié, **visé 48 heures**
Notification à la CNIL, pour les traitements dont Opti' est responsable	72 heures (RGPD, article 33)
Information des personnes, si le risque est élevé	sans retard injustifié (article 34)

Pour les données qu'une organisation collecte dans Opti', c'est elle qui est responsable de traitement : Opti' la prévient, et la notification à l'autorité lui revient.

15 L'exploitation du service

Opti' est édité et exploité par une seule personne, qui détient seule les accès d'administration. Ces accès sont protégés ainsi :

- **Double authentification** sur tous les comptes d'administration : le compte qui ouvre les consoles des hébergeurs, le compte Microsoft, le dépôt de code, le compte de l'éditeur dans Opti'.
- **Codes de secours et clés de récupération** sur papier, hors ligne ; disque du poste de travail chiffré.
- **Secrets** : jamais transmis par messagerie ni écrits dans un document ; collés directement dans la console qui les consomme ; une clé supposée exposée est remplacée, puis l'ancienne révoquée.
- **Assistant de développement** : le code est écrit et audité avec l'aide d'un assistant d'IA (Claude Code). Il lit la base de production en **lecture seule**, par un jeton limité ; il ne lit pas les fichiers de secrets ; toute mise en ligne et toute modification de la base passent par une commande versionnée que l'éditeur autorise.
- **Revue trimestrielle des accès** : membres de chaque console, jetons et leurs échéances, applications tierces autorisées, procédure d'urgence.

16 Limites à connaître

Ce qu'Opti' ne garantit pas à ce jour, à prendre en compte dans une évaluation.

Limite	Ce qu'il faut en retenir
Une seule personne exploite le service	pas de relecture du code par une seconde personne (les contrôles automatiques de la section 13 s'appliquent à chaque modification) ; pas de surveillance continue des journaux, qui sont lus à la main ; une procédure d'urgence couvre l'indisponibilité de l'éditeur
Pas de certification ni d'évaluation externe	ni ISO 27001, ni SOC 2, ni test d'intrusion externe à ce jour ; l'évaluation est interne
Les mots de passe ne sont pas comparés aux listes de mots de passe divulgués	cette vérification demande une offre payante de l'hébergeur de l'authentification ; la double authentification, exigible par l'organisation, couvre ce risque
Pas de durée maximale de session	choix lié au travail hors connexion (section 4)
OptIA transite par les États-Unis	le calcul a lieu en Europe, mais le point d'entrée des requêtes est aux États-Unis
Fondement des transferts hors de l'Union européenne	en cours de relevé fournisseur par fournisseur (section 11)

17 Documents complémentaires

Disponibles sur demande, à l'adresse de contact :

- **Accord de traitement des données** (RGPD, article 28), prêt à signer.
- **Questionnaire de sécurité préremplí**, au format des questionnaires des grandes organisations, chaque réponse renvoyant à sa preuve.
- **Liste des sous-traitants** détaillée, avec garanties et références.
- **Nomenclature logicielle** (CycloneDX) de l'application et du serveur.

En ligne :

- Sécurité d'Opti' et politique de divulgation : myoptibot.com/securite/
- Politique de confidentialité : https://lequeux-thomas.com/addin/site/legal/fr/
- Conditions générales d'utilisation et de vente : https://lequeux-thomas.com/addin/site/termofuse/fr/
- Le cadre TRUST, cinq principes pour une IA compatible avec les exigences humanitaires : myoptibot.com/ia-ethic/
- Notice pour l'administrateur SharePoint : myoptibot.com/sharepoint-administrateur/

Mise à jour. Ce dossier est revu au moins une fois par an et à chaque changement d'architecture ou de fournisseur. La version en ligne fait foi.

A Annexe : conformité à l'OWASP ASVS 5.0.0, niveaux 1 et 2

Chaque exigence des niveaux 1 et 2 de l'OWASP Application Security Verification Standard 5.0.0 (mai 2025), avec son statut pour Opti'. Le niveau 1 est le socle attendu de toute application ; le niveau 2, celui d'une application qui traite des données sensibles. Évaluation interne, exigence par exigence, sur preuve (lecture du code, mesure, essai), mise à jour le 2026-11-16. Les preuves des exigences conformes sont disponibles sur demande.

Niveau	Exigences	Conformes	Partielles	Non conformes	Non applicables	Taux sur les applicables
Niveau 1	70	54	9	1	6	**84 %**
Niveau 2	183	99	27	10	47	**73 %**

Texte des exigences : OWASP Foundation, traduction française officielle, licence CC BY-SA 4.0.

V1 · Encodage et nettoyage

	Niv.	Texte	Statut
V1.1.1	2	Vérifiez que l'entrée est décodée ou non échappée vers une forme canonique une seule fois, elle n'est décodée que lorsque des données codées sous cette forme sont attendues, et que cela est fait avant de traiter davantage l'entrée, par exemple, elle n'est pas effectuée après la validation ou la désinfection de l'entrée.	Conforme
V1.1.2	2	Vérifiez que l'application effectue l'encodage et l'échappement de sortie soit comme étape finale avant d'être utilisée par l'interpréteur pour lequel elle est destinée, soit par l'interpréteur lui-même.	Conforme
V1.2.1	1	Vérifiez que l'encodage de sortie d'une réponse HTTP, d'un document HTML ou d'un document XML est pertinent pour le contexte requis, comme l'encodage des caractères pertinents pour les éléments HTML, les attributs HTML, les commentaires HTML, les CSS ou les champs d'en-tête HTTP, pour éviter de modifier la structure du message ou du document. *Le texte affiché est échappé avant d'être inséré dans la page ; les surfaces alimentées par un tiers ont été revues et corrigées. La revue de l'ensemble du code n'est pas terminée.*	Partiel
V1.2.2	1	Vérifiez que, lors de la création dynamique d'URL, les données non fiables sont encodées en fonction de leur contexte (par exemple, encodage d'URL ou encodage base64url pour les paramètres de requête ou de chemin). Assurez-vous que seuls les schémas d'URL sûrs sont autorisés (par exemple, interdire javascript: ou data:).	Conforme
V1.2.3	1	Vérifiez que l'encodage ou l'échappement de sortie est utilisé lors de la création dynamique de contenu JavaScript (y compris JSON), pour éviter de modifier la structure du message ou du document (pour éviter l'injection JavaScript et JSON).	Conforme
V1.2.4	1	Vérifiez que la sélection de données ou les requêtes de base de données (par exemple, SQL, HQL, NoSQL, Cypher) utilisent des requêtes paramétrées, des ORM, des Framework d'entités ou sont protégées contre les injections SQL et autres attaques par injection de base de données. Ceci est également pertinent lors de l'écriture de procédures stockées.	Conforme
V1.2.5	1	Vérifiez que l'application protège contre l'injection de commandes du système d'exploitation et que les appels du système d'exploitation utilisent des requêtes du système d'exploitation paramétrées ou utilisent un encodage de sortie de ligne de commande contextuelle.	Conforme
V1.2.6	2	Vérifiez que l'application protège contre les vulnérabilités d'injection LDAP ou que des contrôles de sécurité spécifiques pour empêcher l'injection LDAP ont été mis en œuvre. *Aucun annuaire LDAP.*	Non applicable
V1.2.7	2	Vérifiez que l'application est protégée contre les attaques par injection XPath en utilisant la paramétrisation des requêtes ou des requêtes précompilées. *Aucune requête XPath sur un document XML. Les expressions des questionnaires (syntaxe ODK) sont évaluées par un analyseur propre, sur les réponses.*	Non applicable

	Niv.	Texte	Statut
V1.2.8	2	Vérifiez que les processeurs LaTeX sont configurés de manière sécurisée (par exemple, en n'utilisant pas l'indicateur « --shell-escape ») et qu'une liste d'autorisations de commandes est utilisée pour empêcher les attaques par injection LaTeX. *Aucun processeur LaTeX ; la notation mathématique des réponses du modèle est convertie en texte.*	Non applicable
V1.2.9	2	Vérifiez que l'application échappe les caractères spéciaux dans les expressions régulières (généralement à l'aide d'une barre oblique inverse) pour éviter qu'ils ne soient mal interprétés comme des métacaractères.	Conforme
V1.3.1	1	Vérifiez que toutes les entrées HTML non fiables provenant d'éditeurs WYSIWYG ou similaires sont nettoyées à l'aide d'une bibliothèque ou d'une fonctionnalité de Framework de nettoyage HTML bien connue et sécurisée.	Conforme
V1.3.2	1	Vérifiez que l'application évite d'utiliser eval() ou d'autres fonctionnalités d'exécution de code dynamique telles que Spring Expression Language (SpEL). En l'absence d'alternative, toute saisie utilisateur incluse doit être nettoyée avant d'être exécutée.	Conforme
V1.3.3	2	Vérifiez que les données transmises à un contexte potentiellement dangereux sont préalablement nettoyées pour appliquer des mesures de sécurité, telles qu'autoriser uniquement des caractères sûrs pour ce contexte et raccourcir des entrées trop longues. *Les contextes dangereux relevés (HTML, filtres de base, en-têtes, noms de fichiers) sont traités ; la revue n'est pas exhaustive.*	Partiel
V1.3.4	2	Vérifiez que le contenu Scalable Vector Graphics (SVG) scriptable fourni par l'utilisateur est validé ou nettoyé pour contenir uniquement des balises et des attributs (tels que des graphiques de dessin) qui sont sûrs pour l'application, par exemple, ne contiennent pas de scripts et d'objets étrangers.	Conforme
V1.3.5	2	Vérifiez que l'application nettoie ou désactive le contenu du langage de modèle d'expression ou de script fourni par l'utilisateur, tel que les feuilles de style CSS, le Markdown ou XSL, BBCode ou similaire.	Conforme
V1.3.6	2	Vérifiez que l'application protège contre les attaques de falsification de requête côté serveur (SSRF), en validant les données non fiables par rapport à une liste d'autorisation de protocoles, de domaines, de chemins et de ports et en nettoyant les caractères potentiellement dangereux avant d'utiliser les données pour appeler un autre service.	Conforme
V1.3.7	2	Vérifiez que l'application se protège contre les attaques par injection de modèles en interdisant la création de modèles basés sur des entrées non fiables. En l'absence d'alternative, toute entrée non fiable incluse dynamiquement lors de la création du modèle doit être nettoyée ou rigoureusement validée.	Conforme
V1.3.8	2	Vérifiez que l'application nettoie correctement les entrées non fiables avant utilisation dans les requêtes Java Naming and Directory Interface (JNDI) et que JNDI est configuré de manière sécurisée pour empêcher les attaques par injection JNDI. *Pas de JNDI (Node.js).*	Non applicable
V1.3.9	2	Vérifiez que l'application nettoie le contenu avant qu'il ne soit envoyé à memcache pour éviter les attaques par injection. *Pas de memcache.*	Non applicable
V1.3.10	2	Vérifiez que les chaînes de format susceptibles d'être résolues de manière inattendue ou malveillante lors de leur utilisation sont nettoyées avant d'être traitées. *Pas de chaînes de format interprétées (JavaScript).*	Non applicable
V1.3.11	2	Vérifiez que l'application nettoie les entrées utilisateur avant de les transmettre aux systèmes de messagerie pour se protéger contre l'injection SMTP ou IMAP.	Conforme
V1.4.1	2	Vérifiez que l'application utilise des chaînes memory-safe, une copie de mémoire et une arithmétique de pointeur renforcée pour détecter ou empêcher les débordements de pile, de tampon ou de tas. *JavaScript à mémoire gérée ; le code du modèle tourne dans QuickJS compilé en WebAssembly.*	Non applicable
V1.4.2	2	Vérifiez que les techniques de validation du signe, de la plage et de l'entrée sont utilisées pour éviter les dépassements d'entiers. *Pas d'entiers à taille fixe manipulés à la main ; montants en centimes bornés par le serveur.*	Non applicable

	Niv.	Texte	Statut
V1.4.3	2	Vérifiez que la mémoire et les ressources allouées dynamiquement sont libérées et que les références ou les pointeurs vers la mémoire libérée sont supprimés ou définis à null pour éviter les "dangling pointer" et les vulnérabilités d'utilisation après libération. *Mémoire gérée par le moteur JavaScript.*	Non applicable
V1.5.1	1	Vérifiez que l'application configure les "parser" XML pour utiliser une configuration restrictive et que les fonctionnalités non sûres telles que la résolution d'entités externes sont désactivées pour empêcher les attaques XML eXternal Entity (XXE).	Conforme
V1.5.2	2	Vérifiez que la désérialisation des données non fiables garantit une gestion sécurisée des entrées, par exemple en utilisant une liste d'autorisation de types d'objets ou en limitant les types d'objets définis par le client, afin d'empêcher les attaques par désérialisation. Les mécanismes de désérialisation explicitement définis comme non sécurisés ne doivent pas être utilisés avec des entrées non fiables.	Conforme

V2 · Validation et logique métier

	Niv.	Texte	Statut
V2.1.1	1	Vérifiez que la documentation de l'application définit des règles de validation des entrées pour vérifier la validité des éléments de données par rapport à la structure attendue. Il peut s'agir de formats de données courants tels que des numéros de carte de crédit, des adresses e-mail ou des numéros de téléphone, ou d'un format de données interne.	Conforme
V2.1.2	2	Vérifiez que la documentation de l'application définit comment valider la cohérence logique et contextuelle des éléments de données combinés, par exemple en vérifiant que la banlieue et le code postal correspondent.	Conforme
V2.1.3	2	Vérifiez que les attentes en matière de limites et de validations de la logique métier sont documentées, y compris par utilisateur et globalement dans l'application.	Conforme
V2.2.1	1	Vérifier que les entrées sont validées afin de respecter les attentes métier ou fonctionnelles. Cette validation doit être basée sur une liste de valeurs, de modèles et de plages autorisées, ou sur la comparaison des entrées avec une structure attendue et des limites logiques selon des règles prédéfinies. Pour le niveau 1, cette validation peut se concentrer sur les entrées utilisées pour prendre des décisions métier ou de sécurité spécifiques. À partir du niveau 2, elle doit s'appliquer à toutes les entrées.	Conforme
V2.2.2	1	Vérifiez que l'application est conçue pour appliquer la validation des entrées au niveau d'une couche de service de confiance. Bien que la validation côté client améliore l'ergonomie et doit être encouragée, elle ne doit pas être considérée comme un contrôle de sécurité.	Conforme
V2.2.3	2	Vérifiez que l’application garantit que les combinaisons d’éléments de données associés sont raisonnables selon les règles prédéfinies.	Conforme
V2.3.1	1	Vérifiez que l’application traitera uniquement les flux de logique métier pour le même utilisateur dans l’ordre séquentiel attendu et sans sauter d’étapes.	Conforme
V2.3.2	2	Vérifiez que les limites de la logique métier sont implémentées conformément à la documentation de l'application, afin d'éviter que des failles de la logique métier ne soient pas exploitées.	Conforme
V2.3.3	2	Vérifiez que les transactions sont utilisées au niveau de la logique métier de telle sorte qu'une opération de logique métier réussisse dans son intégralité ou qu'elle soit restaurée à l'état correct précédent. *Les opérations de crédit sont atomiques ; l'attribution d'un paiement mobile enchaîne plusieurs écritures, sécurisées par l'idempotence plutôt que par une transaction unique.*	Partiel
V2.3.4	2	Vérifiez que les mécanismes de verrouillage au niveau de la logique métier sont utilisés pour garantir que les ressources en quantité limitée (telles que les sièges de théâtre ou les créneaux de livraison) ne peuvent pas être réservées deux fois en manipulant la logique de l'application.	Conforme
V2.4.1	2	Vérifiez que des contrôles anti-automatisation sont en place pour protéger contre les appels excessifs aux fonctions d'application qui pourraient conduire à l'exfiltration de données, à la création de données inutiles, à l'épuisement des quotas, aux violations de limites de débit, au déni de service ou à la surutilisation de ressources coûteuses.	Conforme

V3 · Sécurité du frontend Web

	Niv.	Texte	Statut
V3.2.1	1	Vérifiez que des contrôles de sécurité sont en place pour empêcher les navigateurs d'afficher du contenu ou des fonctionnalités dans les réponses HTTP dans un contexte incorrect (par exemple, lorsqu'une API, un fichier téléchargé par l'utilisateur ou une autre ressource est demandée directement). Les contrôles possibles peuvent inclure : ne pas transmettre le contenu sauf si les champs d'en-tête de requête HTTP (tels que Sec-Fetch-*) indiquent qu'il s'agit du contexte correct, utiliser la directive sandbox du champ d'en-tête Content-Security-Policy ou utiliser le type de disposition de pièce jointe dans le champ d'en-tête Content-Disposition. *L'API ne renvoie que du JSON, avec l'en-tête nosniff. L'en-tête de téléchargement des fichiers servis par l'hébergeur de la base n'a pas encore été vérifié.*	Partiel
V3.2.2	1	Vérifiez que le contenu destiné à être affiché sous forme de texte, plutôt que rendu sous forme de HTML, est géré à l'aide de fonctions de rendu sécurisées (telles que createTextNode ou textContent) pour empêcher l'exécution involontaire de contenu tel que HTML ou JavaScript. *Le texte est rendu par échappement plutôt que par les fonctions natives d'affichage de texte ; même protection, forme différente de celle que demande l'exigence.*	Partiel
V3.3.1	1	Vérifiez que les cookies ont l'attribut « Secure » défini et si le préfixe « __Host- » n'est pas utilisé pour le nom du cookie, le préfixe « __Secure- » doit être utilisé pour le nom du cookie. *Aucun cookie posé par le backend ni par les sites (recherche du 2026-11-13) ; la session vit dans le stockage du navigateur.*	Non applicable
V3.3.2	2	Vérifiez que la valeur de l'attribut « SameSite » de chaque cookie est définie en fonction de l'objectif du cookie, afin de limiter l'exposition aux attaques de réparation de l'interface utilisateur et aux attaques de falsification de requêtes basées sur le navigateur, communément appelées falsification de requêtes intersites (CSRF). *Aucun cookie.*	Non applicable
V3.3.3	2	Vérifiez que les cookies ont le préfixe « __Host- » pour le nom du cookie, sauf s'ils sont explicitement conçus pour être partagés avec d'autres hôtes. *Aucun cookie.*	Non applicable
V3.3.4	2	Vérifiez que si la valeur d'un cookie n'est pas censée être accessible aux scripts côté client (comme un jeton de session), le cookie doit avoir l'attribut « HttpOnly » défini et la même valeur (par exemple, un jeton de session) ne doit être transférée au client que via le champ d'en-tête « Set-Cookie ». *Aucun cookie ; le jeton de session vit dans le stockage du navigateur (choix de Supabase), lisible par un script : d'où l'importance de V1.2.1 et V3.4.3.*	Non applicable
V3.4.1	1	Vérifiez qu'un champ d'en-tête Strict-Transport-Security est inclus dans toutes les réponses afin d'appliquer une politique HTTP Strict Transport Security (HSTS). Une durée maximale d'au moins un an doit être définie, et pour les niveaux L2 et supérieurs, la politique doit également s'appliquer à tous les sous-domaines.	Conforme
V3.4.2	1	Vérifiez que le champ d'en-tête Access-Control-Allow-Origin du partage de ressources cross-origine (CORS) est une valeur fixe de l'application ou, si la valeur du champ d'en-tête de requête HTTP Origin est utilisée, qu'elle est validée par rapport à une liste d'origines approuvées. Si « Access-Control-Allow-Origin: * » doit être utilisé, vérifiez que la réponse ne contient aucune information sensible.	Conforme
V3.4.3	2	Vérifiez que les réponses HTTP incluent un champ d'en-tête de réponse Content-Security-Policy qui définit des directives garantissant que le navigateur charge et exécute uniquement du contenu ou des ressources fiables, afin de limiter l'exécution de JavaScript malveillant. Au minimum, une politique globale doit être utilisée, incluant les directives object-src 'none' et base-uri 'none', et définissant soit une lliste d'autorisations, soit des valeurs nonces ou des hachages. Pour une application L3, une politique par réponse avec des valeurs nonces ou des hachages doit être définie. *Politique de sécurité du contenu stricte sur l'application et la page de saisie ; pas encore sur les quelques pages HTML servies par l'API.*	Partiel

	Niv.	Texte	Statut
V3.4.4	2	Vérifiez que toutes les réponses HTTP contiennent un champ d'en-tête « X-Content-Type-Options: nosniff ». Cela indique aux navigateurs de ne pas utiliser l'analyse de contenu ni la détection du type MIME pour la réponse donnée, et d'exiger que la valeur du champ d'en-tête « Content-Type » de la réponse corresponde à la ressource de destination. Par exemple, la réponse à une demande de style n'est acceptée que si le type de contenu de la réponse est « text/css ». Cela permet également au navigateur d'utiliser la fonctionnalité de blocage de lecture inter-origines (CORB). *En-tête nosniff sur l'API et myoptibot.com ; pas encore sur lequeux-thomas.com.*	Partiel
V3.4.5	2	Vérifiez que l'application définit une politique de référencement afin d'empêcher la fuite de données techniquement sensibles vers des services tiers via le champ d'en-tête de requête HTTP « Referer ». Cela peut être effectué via le champ d'en-tête de réponse HTTP « Referrer-Policy » ou via les attributs d'élément HTML. Les données sensibles peuvent inclure le chemin d'accès et les données de requête dans l'URL, et pour les applications internes non publiques, le nom d'hôte.	Conforme
V3.4.6	2	Vérifiez que l'application Web utilise la directive frame-ancestors du champ d'en-tête Content-Security-Policy pour chaque réponse HTTP afin de garantir qu'elle ne peut pas être intégrée par défaut et que l'intégration de ressources spécifiques n'est autorisée qu'en cas de nécessité. Notez que le champ d'en-tête X-Frame-Options, bien que pris en charge par les navigateurs, est obsolète et n'est pas forcément fiable. *Affichage dans le cadre d'un autre site interdit pour l'application, l'API et myoptibot.com ; pas sur lequeux-thomas.com, où le complément Excel doit pouvoir s'afficher dans Office.*	Partiel
V3.5.1	1	Vérifiez que, si l'application ne s'appuie pas sur le mécanisme de requête de pré-vérification cross-origin CORS pour empêcher les requêtes inter-origines non autorisées d'utiliser des fonctionnalités sensibles, ces requêtes sont validées afin de garantir leur origine. Cela peut se faire en utilisant et en validant des jetons anti-falsification ou en exigeant des champs d'en-tête HTTP supplémentaires qui ne sont pas des champs d'en-tête de requête CORS safelist. Ceci permet de se protéger contre les attaques de falsification de requêtes basées sur le navigateur, communément appelées falsification de requêtes intersites (CSRF).	Conforme
V3.5.2	1	Vérifiez que, si l'application s'appuie sur le mécanisme de requête de pré-vérification cross-origin CORS pour empêcher l'utilisation inter-origines non autorisée de fonctionnalités sensibles, il est impossible d'appeler la fonctionnalité avec une requête qui ne déclenche pas de requête de pré-vérification cross-origin CORS. Cela peut nécessiter de vérifier les valeurs des champs d'en-tête de requête 'Origin' et 'Content-Type' ou d'utiliser un champ d'en-tête supplémentaire qui n'est pas un champ d'en-tête de la liste de sécurité CORS.	Conforme
V3.5.3	1	Vérifiez que les requêtes HTTP destinées aux fonctionnalités sensibles utilisent des méthodes HTTP appropriées, telles que POST, PUT, PATCH ou DELETE, et non des méthodes définies comme « sûres » par la spécification HTTP, telles que HEAD, OPTIONS ou GET. Une validation stricte des champs d'en-tête de requête Sec-Fetch-* peut également être utilisée pour garantir que la requête ne provient pas d'un appel inter-origines inapproprié, d'une requête de navigation ou d'un chargement de ressources (comme une source d'image) inattendu.	Conforme
V3.5.4	2	Vérifiez que des applications distinctes sont hébergées sur des noms d'hôte différents pour tirer parti des restrictions fournies par la politique de même origine, y compris la manière dont les documents ou scripts chargés par une origine peuvent interagir avec les ressources d'une autre origine et les restrictions basées sur le nom d'hôte sur les cookies. *L'application partage le nom de domaine du site vitrine ; ce choix permet au site de reconnaître une session ouverte dans l'application.*	Non conforme
V3.5.5	2	Vérifiez que les messages reçus par l'interface postMessage sont rejetés si l'origine du message n'est pas digne de confiance ou si la syntaxe du message n'est pas valide.	Conforme
V3.7.1	2	Vérifiez que l'application utilise uniquement des technologies côté client toujours prises en charge et considérées comme sécurisées. Parmi les technologies qui ne répondent pas à cette exigence figurent les plugins NSAPI, Flash, Shockwave, ActiveX, Silverlight, NACL ou les applets Java côté client.	Conforme
V3.7.2	2	Vérifiez que l'application redirigera automatiquement l'utilisateur vers un nom d'hôte ou un domaine différent (qui n'est pas contrôlé par l'application) uniquement lorsque la destination apparaît sur une liste d'autorisation.	Conforme

V4 · API et service Web

	Niv.	Texte	Statut
V4.1.1	1	Vérifiez que chaque réponse HTTP avec un corps de message contient un champ d'en-tête Content-Type qui correspond au contenu réel de la réponse, y compris le paramètre charset pour spécifier un codage de caractères sécurisé (par exemple, UTF-8, ISO-8859-1) conformément aux types de médias IANA, tels que « text/ », « /+xml » et « /xml ». *Jeu de caractères déclaré sur l'API et sur myoptibot.com ; pas encore sur le site lequeux-thomas.com.*	Partiel
V4.1.2	2	Vérifiez que seuls les terminaux utilisateurs (destinés à l'accès manuel via un navigateur web) redirigent automatiquement de HTTP vers HTTPS, tandis que les autres services ou terminaux n'implémentent pas de redirections transparentes. Cela permet d'éviter qu'un client envoie par erreur des requêtes HTTP non chiffrées, mais que, comme ces requêtes sont automatiquement redirigées vers HTTPS, la fuite de données sensibles passe inaperçue. *La redirection de HTTP vers HTTPS de l'API est faite par l'hébergeur et ne se règle pas.*	Partiel
V4.1.3	2	Vérifiez que tout champ d'en-tête HTTP utilisé par l'application et défini par une couche intermédiaire, telle qu'un équilibreur de charge, un proxy web ou un service backend-for-frontend, ne peut pas être remplacé par l'utilisateur final. Les exemples d'en-têtes peuvent inclure X-Real-IP, X-Forwarded-*, ou X-User-ID.	Conforme
V4.2.1	2	Vérifiez que tous les composants de l'application (y compris les équilibreurs de charge, les pares-feux et les serveurs d'applications) déterminent les limites des messages HTTP entrants à l'aide du mécanisme approprié à la version HTTP afin d'empêcher la contrebande de requêtes HTTP. Dans HTTP/1.x, si un champ d'en-tête Transfer-Encoding est présent, l'en-tête Content-Length doit être ignoré conformément à la RFC 2616. Avec HTTP/2 ou HTTP/3, si un champ d'en-tête Content-Length est présent, le récepteur doit s'assurer qu'il est cohérent avec la longueur des trames DATA.	Conforme
V4.3.1	2	Vérifiez qu'une liste d'autorisation de requête, une limitation de profondeur, une limitation de quantité ou une analyse des coûts de requête est utilisée pour empêcher le déni de service (DoS) de GraphQL ou d'expression de la couche données en raison de requêtes imbriquées coûteuses. *Aucune API GraphQL : l'extension pg_graphql n'est pas installée (mesuré).*	Non applicable
V4.3.2	2	Vérifiez que les requêtes d'introspection GraphQL sont désactivées dans l'environnement de production, sauf si l'API GraphQL est destinée à être utilisée par d'autres parties. *Idem.*	Non applicable
V4.4.1	1	Vérifiez que WebSocket sur TLS (WSS) est utilisé pour toutes les connexions WebSocket.	Conforme
V4.4.2	2	Vérifiez que, lors de la négociation HTTP WebSocket initiale, le champ d'en-tête 'Origin' est vérifié par rapport à une liste d'origines autorisées pour l'application. *Les seules WebSocket sont celles de Supabase Realtime, gérées par le fournisseur.*	Non applicable
V4.4.3	2	Vérifiez que, si la gestion de session standard de l'application ne peut pas être utilisée, des jetons dédiés sont utilisés à cet effet, qui sont conformes aux exigences de sécurité de gestion de session pertinentes. *Idem.*	Non applicable
V4.4.4	2	Vérifiez que les jetons de gestion de session WebSocket dédiés sont initialement obtenus ou validés via la session HTTPS précédemment authentifiée lors de la transition d'une session HTTPS existante vers un canal WebSocket. *Idem.*	Non applicable

V5 · Gestion des fichiers

	Niv.	Texte	Statut
V5.1.1	2	Vérifiez que la documentation définit les types de fichiers autorisés, les extensions de fichiers attendues et la taille maximale (y compris la taille décompressée) pour chaque fonctionnalité de Téléversement. De plus, assurez-vous que la documentation précise comment les fichiers sont sécurisés pour le téléchargement et le traitement des utilisateurs finaux, par exemple le comportement de l'application lorsqu'un fichier malveillant est détecté.	Conforme
V5.2.1	1	Vérifiez que l'application n'acceptera que des fichiers d'une taille qu'elle peut traiter sans provoquer de perte de performances ou d'attaque par déni de service.	Conforme

	Niv.	Texte	Statut
V5.2.2	1	Vérifiez que lorsque l'application accepte un fichier, seul ou dans une archive telle qu'un fichier zip, elle vérifie si l'extension de fichier correspond à une extension attendue et que le contenu correspond au type représenté par l'extension. Cela inclut, sans s'y limiter, la vérification des « octets magiques » initiaux, la réécriture d'images et l'utilisation de bibliothèques spécialisées pour la validation du contenu des fichiers. Pour le niveau L1, cela peut se concentrer uniquement sur les fichiers utilisés pour prendre des décisions métier ou de sécurité spécifiques. À partir du niveau L2, cela doit s'appliquer à tous les fichiers acceptés.	Conforme
V5.2.3	2	Vérifiez que l'application vérifie les fichiers compressés (par exemple, zip, gz, docx, odt) par rapport à la taille maximale autorisée non compressée et au nombre maximal de fichiers avant de décompresser le fichier.	Conforme
V5.3.1	1	Vérifiez que les fichiers téléversés ou générés par une entrée non fiable et stockés dans un dossier public ne sont pas exécutés en tant que code de programme côté serveur lorsqu'ils sont accessibles directement avec une requête HTTP.	Conforme
V5.3.2	1	Vérifiez que lorsque l'application crée des chemins d'accès pour les opérations sur les fichiers, elle utilise des données générées en interne ou fiables plutôt que des noms de fichiers soumis par l'utilisateur. Si des noms de fichiers ou des métadonnées de fichiers soumis par l'utilisateur doivent être utilisés, une validation et un nettoyage stricts doivent être appliqués. Ceci permet de se protéger contre les attaques par traversée de chemin, l'inclusion de fichiers locaux ou distants (LFI, RFI) et la falsification de requêtes côté serveur (SSRF).	Conforme
V5.4.1	2	Vérifiez que l'application valide ou ignore les noms de fichiers soumis par l'utilisateur, y compris dans un paramètre JSON, JSONP ou URL et spécifie un nom de fichier dans le champ d'en-tête Content-Disposition de la réponse. *Les fichiers servis portent un nom fixé par le serveur ; les noms de fichiers envoyés ne sont jamais réutilisés tels quels.*	Partiel
V5.4.2	2	Vérifiez que les noms de fichiers servis (par exemple, dans les champs d'en-tête de réponse HTTP ou les pièces jointes aux e-mails) sont encodés ou nettoyés (par exemple, conformément à la RFC 6266) pour préserver la structure du document et empêcher les attaques par injection.	Conforme
V5.4.3	2	Vérifiez que les fichiers obtenus à partir de sources non fiables sont analysés par des scanners antivirus pour empêcher la diffusion de contenu malveillant connu. *Pas d'antivirus sur les fichiers reçus (photos des réponses, pièces jointes Kobo) ; ils ne sont montrés qu'au propriétaire de la collecte.*	Non conforme

V6 · Authentification

	Niv.	Texte	Statut
V6.1.1	1	Vérifiez que la documentation de l'application définit comment les contrôles, tels que la limitation de débit, l'anti-automatisation et la réponse adaptative, sont utilisés pour se défendre contre les attaques telles que le « credential stuffing » et la force brute des mots de passe. La documentation doit expliquer clairement comment ces contrôles sont configurés et empêcher le blocage malveillant des comptes.	Conforme
V6.1.2	2	Vérifiez qu'une liste de mots spécifiques au contexte est documentée afin d'empêcher leur utilisation dans les mots de passe. Cette liste peut inclure des permutations de noms d'organisations, de produits, d'identifiants de systèmes, de noms de codes de projets, de noms de services ou de rôles, etc. *Pas de liste de mots propres au contexte (nom du produit…) interdits dans les mots de passe.*	Non conforme
V6.1.3	2	Vérifiez que, si l'application inclut plusieurs voies d'authentification, celles-ci sont toutes documentées avec les contrôles de sécurité et la force d'authentification qui doivent être appliqués de manière cohérente.	Conforme
V6.2.1	1	Vérifiez que les mots de passe définis par l'utilisateur comportent au moins 8 caractères, bien qu'un minimum de 15 caractères soit fortement recommandé.	Conforme
V6.2.2	1	Vérifiez que les utilisateurs peuvent modifier leur mot de passe.	Conforme
V6.2.3	1	Vérifiez que la fonctionnalité de changement de mot de passe nécessite le mot de passe actuel et le nouveau mot de passe de l'utilisateur. *Un changement de mot de passe demande une reconnexion si la session a plus de 24 heures ; le mot de passe actuel n'est pas redemandé dans tous les cas.*	Partiel

	Niv.	Texte	Statut
V6.2.4	1	Vérifiez que les mots de passe soumis lors de l'enregistrement du compte ou du changement de mot de passe sont vérifiés par rapport à un ensemble disponible d'au moins 3 000 mots de passe principaux qui correspondent à la politique de mot de passe de l'application, par exemple la longueur minimale. *Les mots de passe ne sont pas comparés à une liste de mots de passe courants : la fonction de l'hébergeur de l'authentification est réservée à son offre payante. La double authentification, exigible par l'organisation, couvre ce risque.*	Non conforme
V6.2.5	1	Vérifiez que les mots de passe peuvent être utilisés, quelle que soit leur composition, sans restriction quant au type de caractères autorisés. Aucun nombre minimal de majuscules ou de minuscules, de chiffres ou de caractères spéciaux ne doit être exigé.	Conforme
V6.2.6	1	Vérifiez que les champs de saisie du mot de passe utilisent type=password pour masquer la saisie. Les applications peuvent permettre à l'utilisateur d'afficher temporairement l'intégralité du mot de passe masqué ou le dernier caractère saisi.	Conforme
V6.2.7	1	Vérifiez que la fonctionnalité « coller », les assistants de mot de passe du navigateur et les gestionnaires de mots de passe externes sont autorisés.	Conforme
V6.2.8	1	Vérifiez que l'application vérifie le mot de passe de l'utilisateur exactement tel qu'il a été reçu de l'utilisateur, sans aucune modification telle qu'une troncature ou une transformation de casse.	Conforme
V6.2.9	2	Vérifiez que les mots de passe d'au moins 64 caractères sont autorisés. *Les mots de passe longs sont acceptés ; la limite de l'hébergeur de l'authentification est de 72 octets, soit moins de 64 caractères accentués.*	Partiel
V6.2.10	2	Vérifiez que le mot de passe d'un utilisateur reste valide jusqu'à ce qu'il soit découvert comme compromis ou qu'il soit renouvelé. L'application ne doit pas exiger de renouvellement périodique des identifiants.	Conforme
V6.2.11	2	Vérifiez que la liste documentée de mots spécifiques au contexte est utilisée pour éviter la création de mots de passe faciles à deviner. *Même écart que V6.1.2.*	Non conforme
V6.2.12	2	Vérifiez que les mots de passe soumis lors de l'enregistrement du compte ou des modifications de mot de passe sont vérifiés par rapport à un ensemble de mots de passe fuités. *Comparaison aux mots de passe divulgués réservée à l'offre payante de l'hébergeur de l'authentification ; même compensation que V6.2.4.*	Non conforme
V6.3.1	1	Vérifiez que les contrôles visant à empêcher les attaques telles que le bourrage d'informations d'identification et la force brute des mots de passe sont mis en œuvre conformément à la documentation de sécurité de l'application.	Conforme
V6.3.2	1	Vérifiez que les comptes d'utilisateur par défaut (par exemple, « root », « admin » ou « sa ») ne sont pas présents dans l'application ou sont désactivés.	Conforme
V6.3.3	2	Vérifiez que l'application exige que les utilisateurs utilisent un mécanisme d'authentification multifacteur ou une combinaison de mécanismes d'authentification à facteur unique. *Double authentification disponible pour tous, et exigible par une organisation pour ses membres ; elle n'est pas imposée à chaque compte individuel.*	Partiel
V6.3.4	2	Vérifiez que, si l'application inclut plusieurs voies d'authentification, il n'existe aucune voie non documentée et que les contrôles de sécurité et la force d'authentification sont appliqués de manière cohérente. *Toutes les voies de connexion produisent la même session et exigent le second facteur quand il est dû ; les réglages côté LinkedIn restent à relire.*	Partiel
V6.4.1	1	Vérifiez que les mots de passe initiaux ou les codes d'activation générés par le système sont générés de manière aléatoire et sécurisée, qu'ils respectent la politique de mots de passe en vigueur et qu'ils expirent après une courte période ou après leur première utilisation. Ces secrets initiaux ne doivent pas devenir des mots de passe permanents.	Conforme
V6.4.2	1	Vérifiez que les indices de mot de passe ou l'authentification basée sur les connaissances (appelées « questions secrètes ») ne sont pas présents.	Conforme
V6.4.3	2	Vérifiez qu'un processus sécurisé de réinitialisation d'un mot de passe oublié est mis en œuvre, qui ne contourne aucun mécanisme d'authentification multifacteur activé.	Conforme

	Niv.	Texte	Statut
V6.4.4	2	Vérifiez que si un facteur d'authentification multifacteur est perdu, la preuve de vérification d'identité est effectuée au même niveau que lors de l'inscription.	Conforme
V6.5.1	2	Vérifiez que les secrets de recherche, les demandes ou codes d'authentification out-of-band et les mots de passe à usage unique basés sur le temps (TOTP) ne peuvent être utilisés avec succès qu'une seule fois.	Conforme
V6.5.2	2	Vérifiez que, lors de leur stockage dans le backend de l'application, les secrets de recherche comportant moins de 112 bits d'entropie (19 caractères alphanumériques aléatoires ou 34 chiffres aléatoires) sont hachés avec un algorithme de hachage de stockage de mots de passe approuvé, intégrant un sel aléatoire de 32 bits. Une fonction de hachage standard peut être utilisée si le secret comporte 112 bits d'entropie ou plus.	Conforme
V6.5.3	2	Vérifiez que les secrets de recherche, le code d'authentification out-of-band et les mots de passe à usage unique basés sur le temps sont générés à l'aide d'un générateur de nombres pseudo-aléatoires cryptographiquement sécurisé (CSPRNG) pour éviter les valeurs prévisibles.	Conforme
V6.5.4	2	Vérifiez que les secrets de recherche et les codes d'authentification out-of-band ont un minimum de 20 bits d'entropie (généralement 4 caractères alphanumériques aléatoires ou 6 chiffres aléatoires suffisent).	Conforme
V6.5.5	2	Vérifiez que les requêtes, codes ou jetons d'authentification out-of-band, ainsi que les mots de passe à usage unique (TOTP), ont une durée de vie définie. Les requêtes out-of-band doivent avoir une durée de vie maximale de 10 minutes et les TOTP, de 30 secondes.	Conforme
V6.6.1	2	Vérifier que les mécanismes d'authentification utilisant le réseau téléphonique public commuté (RTPC) pour la transmission de mots de passe à usage unique (OTP) par téléphone ou SMS ne sont proposés que lorsque le numéro de téléphone a été préalablement validé. D'autres méthodes plus robustes (telles que les mots de passe à usage unique à durée déterminée) sont également proposées, et que le service informe les utilisateurs des risques de sécurité qu'elles présentent. Pour les applications de niveau 3, le téléphone et les SMS ne doivent pas être disponibles. *Aucune connexion par SMS ou téléphone.*	Non applicable
V6.6.2	2	Vérifiez que les demandes d'authentification out-of-band, les codes ou les jetons sont liés à la demande d'authentification d'origine pour laquelle ils ont été générés et ne sont pas utilisables pour une demande précédente ou ultérieure.	Conforme
V6.6.3	2	Vérifiez qu'un mécanisme d'authentification out-of-band basé sur du code est protégé contre les attaques par force brute grâce au "rate limiting". Envisagez également d'utiliser un code avec au moins 64 bits d'entropie.	Conforme
V6.8.1	2	Vérifiez que, si l'application prend en charge plusieurs fournisseurs d'identité (IdP), l'identité de l'utilisateur ne peut pas être usurpée via un autre fournisseur d'identité pris en charge (par exemple, en utilisant le même identifiant utilisateur). La mesure standard consisterait à ce que l'application enregistre et identifie l'utilisateur à l'aide d'une combinaison de l'ID du fournisseur d'identité (servant d'espace de noms) et de l'ID de l'utilisateur dans le fournisseur d'identité.	Conforme
V6.8.2	2	Vérifiez que la présence et l'intégrité des signatures numériques sur les assertions d'authentification (par exemple sur les assertions JWT ou SAML) sont toujours validées, en rejetant toutes les assertions non signées ou ayant des signatures non valides.	Conforme
V6.8.3	2	Vérifiez que les assertions SAML sont traitées de manière unique et utilisées une seule fois au cours de la période de validité pour éviter les attaques par rejeu. *Aucun SAML.*	Non applicable
V6.8.4	2	Si une application utilise un fournisseur d'identité (IdP) distinct et attend une force, des méthodes ou une date d'authentification spécifiques pour des fonctions spécifiques, vérifiez que l'application les vérifie à l'aide des informations renvoyées par l'IdP. Par exemple, si OIDC est utilisé, cela peut être réalisé en validant les affirmations de jeton d'identification telles que « acr », « amr » et « auth_time » (le cas échéant). Si l'IdP ne fournit pas ces informations, l'application doit disposer d'une approche de secours documentée qui suppose que le mécanisme d'authentification de force minimale a été utilisé (par exemple, une authentification à facteur unique avec nom d'utilisateur et mot de passe). *Aucune fonction ne dépend de la méthode d'authentification utilisée.*	Non applicable

V7 · Gestion des sessions

	Niv.	Texte	Statut
V7.1.1	2	Vérifiez que le délai d'inactivité de la session de l'utilisateur et la durée de vie maximale absolue de la session sont documentés, sont appropriés en combinaison avec d'autres contrôles et que la documentation inclut une justification de tout écart par rapport aux exigences de réauthentification NIST SP 800-63B.	Conforme
V7.1.2	2	Vérifiez que la documentation définit le nombre de sessions simultanées (parallèles) autorisées pour un compte ainsi que les comportements et actions prévus à entreprendre lorsque le nombre maximal de sessions actives est atteint.	Conforme
V7.1.3	2	Vérifiez que tous les systèmes qui créent et gèrent des sessions utilisateur dans le cadre d'un écosystème de gestion des identités fédérées (tels que les systèmes SSO) sont documentés avec des contrôles pour coordonner la durée de vie des sessions, la résiliation et toute autre condition nécessitant une réauthentification. *Pas d'écosystème fédéré au-delà de la connexion par fournisseur externe ; la session est celle de Supabase.*	Non applicable
V7.2.1	1	Vérifiez que l'application effectue toutes les vérifications des jetons de session à l'aide d'un service backend de confiance.	Conforme
V7.2.2	1	Vérifiez que l'application utilise des jetons autonomes ou de référence générés dynamiquement pour la gestion des sessions, c'est-à-dire sans utiliser de secrets et de clés d'API statiques.	Conforme
V7.2.3	1	Vérifiez que si des jetons par référence sont utilisés pour représenter les sessions utilisateur, ils sont uniques et générés à l'aide d'un générateur de nombres pseudo-aléatoires cryptographiquement sécurisé (CSPRNG) et possèdent au moins 128 bits d'entropie.	Conforme
V7.2.4	1	Vérifiez que l'application génère un nouveau jeton de session lors de l'authentification de l'utilisateur, y compris la réauthentification, et met fin au jeton de session actuel.	Conforme
V7.3.1	2	Vérifiez qu'il existe un délai d'inactivité tel que la réauthentification soit appliquée conformément à l'analyse des risques et aux décisions de sécurité documentées. *Pas de fermeture des sessions inactives : choix lié au travail hors connexion sur le terrain, et réglage réservé à l'offre payante de l'hébergeur.*	Non conforme
V7.3.2	2	Vérifiez qu'il existe une durée de vie maximale absolue de la session de sorte que la réauthentification soit appliquée conformément à l'analyse des risques et aux décisions de sécurité documentées. *Pas de durée de vie maximale des sessions, pour la même raison.*	Non conforme
V7.4.1	1	Vérifiez que lorsque la fin de session est déclenchée (par exemple, déconnexion ou expiration), l'application interdit toute utilisation ultérieure de la session. Pour les jetons par référence ou les sessions avec état, cela implique l'invalidation des données de session au niveau du backend de l'application. Les applications utilisant des jetons autonomes nécessiteront une solution, comme la gestion d'une liste des jetons terminés, l'interdiction des jetons produits avant une date et une heure spécifique à chaque utilisateur ou la rotation d'une clé de signature spécifique à chaque utilisateur. *La déconnexion révoque la session côté serveur ; le jeton d'accès déjà émis reste accepté par la base jusqu'à son expiration (une heure au plus).*	Partiel
V7.4.2	1	Vérifiez que l'application met fin à toutes les sessions actives lorsqu'un compte utilisateur est désactivé ou supprimé (par exemple, lorsqu'un employé quitte l'entreprise). *La suppression d'un compte supprime ses sessions ; même réserve d'une heure au plus sur le jeton d'accès déjà émis.*	Partiel
V7.4.3	2	Vérifiez que l'application offre la possibilité de mettre fin à toutes les autres sessions actives après une modification ou une suppression réussie de tout facteur d'authentification (y compris la modification du mot de passe via une réinitialisation ou une récupération et, le cas échéant, une mise à jour des paramètres MFA).	Conforme
V7.4.4	2	Vérifiez que toutes les pages nécessitant une authentification disposent d'un accès facile et visible à la fonctionnalité de déconnexion.	Conforme
V7.4.5	2	Vérifiez que les administrateurs d'applications sont en mesure de mettre fin aux sessions actives pour un utilisateur individuel ou pour tous les utilisateurs. *La fermeture des sessions d'un compte par l'éditeur se fait depuis la console de l'hébergeur, pas depuis l'outil d'administration d'Opti'.*	Partiel

	Niv.	Texte	Statut
V7.5.1	2	Vérifiez que l'application nécessite une réauthentification complète avant d'autoriser les modifications des attributs de compte sensibles qui peuvent affecter l'authentification, tels que l'adresse e-mail, le numéro de téléphone, la configuration MFA ou d'autres informations utilisées dans la récupération de compte. *Retirer un second facteur exige une session qui l'a passé ; le changement de mot de passe suit la réserve de V6.2.3 ; le changement d'adresse e-mail n'est pas proposé.*	Partiel
V7.5.2	2	Vérifiez que les utilisateurs peuvent afficher et (après s'être authentifiés à nouveau avec au moins un facteur) terminer une ou toutes les sessions actuellement actives. *Un utilisateur ne peut pas encore voir ni fermer lui-même ses sessions ouvertes ; il peut fermer toutes les autres après un changement de mot de passe.*	Non conforme
V7.6.1	2	Vérifiez que la durée de vie et la fin de la session entre les parties de confiance (RP) et les fournisseurs d'identité (IdP) se comportent comme documenté, en exigeant une réauthentification si nécessaire, par exemple lorsque le temps maximal entre les événements d'authentification IdP est atteint. *Les fournisseurs externes ne servent qu'à ouvrir une session Supabase ; pas de session partagée à synchroniser.*	Non applicable
V7.6.2	2	Vérifiez que la création d'une session nécessite soit le consentement de l'utilisateur, soit une action explicite, empêchant ainsi la création de nouvelles sessions d'application sans interaction de l'utilisateur.	Conforme

V8 · Autorisation

	Niv.	Texte	Statut
V8.1.1	1	Vérifiez que la documentation d'autorisation définit des règles de restriction de l'accès au niveau de la fonction et aux données en fonction des autorisations du consommateur et des attributs des ressources.	Conforme
V8.1.2	2	Vérifiez que la documentation d'autorisation définit les règles de restriction d'accès au niveau des champs (lecture et écriture) en fonction des autorisations des consommateurs et des attributs des ressources. Notez que ces règles peuvent dépendre d'autres valeurs d'attributs de l'objet de données concerné, telles que l'état ou le statut.	Conforme
V8.2.1	1	Vérifiez que l'application garantit que l'accès basé sur la fonction est limité aux consommateurs disposant d'autorisations explicites.	Conforme
V8.2.2	1	Vérifiez que l'application garantit que l'accès spécifique aux données est limité aux consommateurs disposant d'autorisations explicites sur des éléments de données spécifiques afin d'atténuer les références d'objet directes non sécurisées (IDOR) et les autorisations de niveau d'objet rompues (BOLA).	Conforme
V8.2.3	2	Vérifiez que l'application garantit que l'accès au niveau du champ est limité aux consommateurs disposant d'autorisations explicites sur des champs spécifiques afin d'atténuer les problèmes d'autorisation au niveau de la propriété d'objet (BOPLA).	Conforme
V8.3.1	1	Vérifier que l'application applique les règles d'autorisations au niveau de la couche service de confiance et ne s'appuie pas sur des contrôles qu'un consommateur non approuvé pourrait manipuler, comme JavaScript côté client.	Conforme
V8.4.1	2	Vérifiez que les applications multi-tenants utilisent des contrôles inter-tenants pour garantir que les opérations des consommateurs n'affecteront jamais les tenants avec lesquels ils ne sont pas autorisés à interagir.	Conforme

V9 · Jetons autonomes

	Niv.	Texte	Statut
V9.1.1	1	Vérifiez que les jetons autonomes sont validés à l'aide de leur signature numérique ou MAC pour les protéger contre toute falsification avant d'accepter le contenu du jeton.	Conforme

	Niv.	Texte	Statut
V9.1.2	1	Vérifiez que seuls les algorithmes d'une liste d'autorisations peuvent être utilisés pour créer et vérifier des jetons autonomes, dans un contexte donné. La liste d'autorisation doit inclure les algorithmes autorisés, idéalement symétriques ou asymétriques, et ne doit pas inclure l'algorithme « Aucun ». Si les algorithmes symétriques et asymétriques doivent être pris en charge, des contrôles supplémentaires seront nécessaires pour éviter toute confusion de clés.	Conforme
V9.1.3	1	Vérifiez que les clés utilisées pour valider les jetons autonomes proviennent de sources préconfigurées et fiables pour l'émetteur du jeton, empêchant ainsi les attaquants de spécifier des sources et des clés non fiables. Pour les JWT et autres structures JWS, les en-têtes tels que « jku », « x5u » et « jwk » doivent être validés par rapport à une liste d'autorisation de sources fiables.	Conforme
V9.2.1	1	Vérifiez que, si une période de validité est indiquée dans les données du jeton, celui-ci et son contenu ne sont acceptés que si la date de vérification est comprise dans cette période. Par exemple, pour les JWT, les déclarations « nbf » et « exp » doivent être vérifiées.	Conforme
V9.2.2	2	Vérifiez que le service recevant un jeton valide le type de jeton et son utilisation avant d'en accepter le contenu. Par exemple, seuls les jetons d'accès peuvent être acceptés pour les décisions d'autorisation, et seuls les jetons d'identification peuvent être utilisés pour prouver l'authentification des utilisateurs.	Conforme
V9.2.3	2	Vérifiez que le service accepte uniquement les jetons destinés à être utilisés avec ce service (audience). Pour les JWT, cela peut être réalisé en validant la déclaration « aud » par rapport à une liste d'autorisation définie dans le service.	Conforme
V9.2.4	2	Si un émetteur de jetons utilise la même clé privée pour émettre des jetons destinés à différentes audiences, vérifiez que les jetons émis contiennent une restriction d'audience identifiant de manière unique les audiences visées. Cela empêchera la réutilisation d'un jeton avec une audience non prévue. Si l'identifiant d'audience est provisionné dynamiquement, l'émetteur de jetons doit valider ces audiences afin de garantir qu'elles n'entraînent pas d'usurpation d'identité.	Conforme

V10 · Oauth et OIDC

	Niv.	Texte	Statut
V10.1.1	2	Vérifiez que les jetons sont envoyés uniquement aux composants qui en ont absolument besoin. Par exemple, lors de l'utilisation d'un modèle backend-for-frontend pour les applications JavaScript basées sur un navigateur, les jetons d'accès et d'actualisation ne doivent être accessibles qu'au backend. *Les jetons de longue durée de Google et Microsoft restent sur le serveur ; les jetons d'accès courts descendent au navigateur, qui écrit lui-même dans l'espace de l'organisation.*	Partiel
V10.1.2	2	Vérifiez que le client n'accepte les valeurs du serveur d'autorisation (telles que le code d'autorisation ou le jeton d'identification) que si elles résultent d'un flux d'autorisation initié par la même session d'agent utilisateur et la même transaction. Cela nécessite que les secrets générés par le client, tels que la clé de preuve pour l'échange de codes (PKCE) « code_verifier », « state » ou le nonce OIDC, ne puissent être devinés, soient spécifiques à la transaction et soient liés de manière sécurisée au client et à la session d'agent utilisateur au cours de laquelle la transaction a été initiée.	Conforme
V10.2.1	2	Vérifiez que, si le flux de code est utilisé, le client OAuth dispose d'une protection contre les attaques de falsification de requêtes basées sur le navigateur, communément appelées falsification de requêtes intersites (CSRF), qui déclenchent des demandes de jetons, soit en utilisant la fonctionnalité de clé de preuve pour l'échange de code (PKCE), soit en vérifiant le paramètre « state » envoyé dans la demande d'autorisation.	Conforme
V10.2.2	2	Vérifiez que, si le client OAuth peut interagir avec plusieurs serveurs d'autorisation, il dispose d'une protection contre les attaques par confusion. Par exemple, il peut exiger que le serveur d'autorisation renvoie la valeur du paramètre « iss » et la valide dans la réponse d'autorisation et la réponse du jeton.	Conforme
V10.3.1	2	Vérifiez que le serveur de ressources accepte uniquement les jetons d'accès destinés à être utilisés avec ce service (audience). L'audience peut être incluse dans un jeton d'accès structuré (comme la déclaration « aud » dans JWT) ou vérifiée à l'aide du endpoint d'introspection de jeton.	Conforme
V10.3.2	2	Vérifiez que le serveur de ressources applique les décisions d'autorisation en fonction des déclarations du jeton d'accès définissant l'autorisation déléguée. Si des déclarations telles que « sub », « scope » et « authorization_details » sont présentes, elles doivent être prises en compte dans la décision.	Conforme

	Niv.	Texte	Statut
V10.3.3	2	Vérifiez que si une décision de contrôle d'accès nécessite l'identification d'un utilisateur unique à partir d'un jeton d'accès (JWT ou réponse d'introspection de jeton associé), le serveur de ressources identifie l'utilisateur à partir de déclarations non ré attribuables à d'autres utilisateurs. En général, cela implique l'utilisation d'une combinaison de déclarations « iss » et « sub ».	Conforme
V10.3.4	2	Si le serveur de ressources requiert une force d'authentification, des méthodes ou une date d'expiration spécifiques, vérifiez que le jeton d'accès présenté respecte ces contraintes. Par exemple, s'il est présent, utilisez les déclarations OIDC « acr », « amr » et « auth_time » respectivement. *Aucune fonction n'exige une force d'authentification particulière.*	Non applicable
V10.4.1	1	Vérifiez que le serveur d'autorisation valide les URI de redirection en fonction d'une liste d'autorisation spécifique au client d'URI préenregistrés à l'aide d'une comparaison de chaînes exacte. *Opti' n'est pas un serveur d'autorisation (Supabase Auth, Google et Microsoft le sont).*	Non applicable
V10.4.2	1	Vérifiez que, si le serveur d'autorisation renvoie le code d'autorisation dans la réponse, celui-ci ne peut être utilisé qu'une seule fois pour une demande de jeton. Pour la deuxième demande valide avec un code d'autorisation déjà utilisé pour émettre un jeton d'accès, le serveur d'autorisation doit rejeter la demande de jeton et révoquer tous les jetons émis liés au code d'autorisation. *Idem.*	Non applicable
V10.4.3	1	Vérifiez que le code d'autorisation est de courte durée. La durée de vie maximale peut atteindre 10 minutes pour les applications L1 et L2 et 1 minute pour les applications L3. *Idem.*	Non applicable
V10.4.4	1	Vérifiez que, pour un client donné, le serveur d'autorisation autorise uniquement l'utilisation des autorisations nécessaires à ce client. Notez que les autorisations « token » (flux implicite) et « password » (flux d'informations d'identification du propriétaire de la ressource) ne doivent plus être utilisées. *Idem.*	Non applicable
V10.4.5	1	Vérifiez que le serveur d'autorisation atténue les attaques par rejeu de jetons d'actualisation pour les clients publics, de préférence en utilisant des jetons d'actualisation limités par l'expéditeur, par exemple des jetons DPoP (Demonstrating Proof of Possession) ou des jetons d'accès liés à un certificat utilisant le protocole TLS mutuel (mTLS). Pour les applications L1 et L2, la rotation des jetons d'actualisation peut être utilisée. Si cette rotation est utilisée, le serveur d'autorisation doit invalider le jeton d'actualisation après utilisation et révoquer tous les jetons d'actualisation de cette autorisation si un jeton d'actualisation déjà utilisé et invalidé est fourni. *Idem.*	Non applicable
V10.4.6	2	Vérifiez que, si l'octroi de code est utilisé, le serveur d'autorisation atténue les attaques par interception de code en exigeant une clé de preuve pour l'échange de code (PKCE). Pour les demandes d'autorisation, le serveur d'autorisation doit exiger une valeur « code_challenge » valide et ne doit pas accepter une valeur « plain » pour « code_challenge_method ». Pour une demande de jeton, il doit exiger la validation du paramètre « code_verifier ». *Opti' n'est pas serveur d'autorisation (Supabase Auth, Google et Microsoft le sont).*	Non applicable
V10.4.7	2	Vérifiez que si le serveur d'autorisation prend en charge l'enregistrement dynamique des clients non authentifiés, il réduit le risque d'applications clientes malveillantes. Il doit valider les métadonnées clientes, telles que les URI enregistrés, garantir le consentement de l'utilisateur et l'avertir avant de traiter une demande d'autorisation avec une application cliente non approuvée. *Opti' n'est pas serveur d'autorisation (Supabase Auth, Google et Microsoft le sont).*	Non applicable
V10.4.8	2	Vérifiez que les jetons d'actualisation ont une expiration absolue, y compris si l'expiration du jeton d'actualisation glissant est appliquée. *Opti' n'est pas serveur d'autorisation (Supabase Auth, Google et Microsoft le sont).*	Non applicable
V10.4.9	2	Vérifiez que les jetons d'actualisation et les jetons d'accès de référence peuvent être révoqués par un utilisateur autorisé à l'aide de l'interface utilisateur du serveur d'autorisation, afin d'atténuer le risque de clients malveillants ou de jetons volés. *Opti' n'est pas serveur d'autorisation (Supabase Auth, Google et Microsoft le sont).*	Non applicable
V10.4.10	2	Vérifiez que le client confidentiel est authentifié pour les demandes de back-channel client-serveur autorisé telles que les demandes de jeton, les demandes d'autorisation poussée (PAR) et les demandes de révocation de jeton. *Opti' n'est pas serveur d'autorisation (Supabase Auth, Google et Microsoft le sont).*	Non applicable

	Niv.	Texte	Statut
V10.4.11	2	Vérifiez que le client confidentiel est authentifié pour les demandes de back-channel client-serveur autorisé telles que les demandes de jeton, les demandes d'autorisation poussée (PAR) et les demandes de révocation de jeton. *Opti' n'est pas serveur d'autorisation (Supabase Auth, Google et Microsoft le sont).*	Non applicable
V10.5.1	2	Vérifiez que le client (en tant que partie utilisatrice) atténue les attaques par rejeu de jeton d'identification. Par exemple, en vous assurant que la valeur « nonce » du jeton d'identification correspond à la valeur « nonce » envoyée dans la demande d'authentification au fournisseur OpenID (appelée demande d'autorisation envoyée au serveur d'autorisation dans OAuth2). *Opti' n'est pas partie utilisatrice OIDC : la connexion par LinkedIn et Facebook est traitée par Supabase Auth, l'app ne reçoit que la session Supabase.*	Non applicable
V10.5.2	2	Vérifiez que le client identifie de manière unique l'utilisateur à partir des déclarations de jeton d'identification, généralement la déclaration « sub », qui ne peut pas être réaffectée à d'autres utilisateurs (pour la portée d'un fournisseur d'identité). *Opti' n'est pas partie utilisatrice OIDC : la connexion par LinkedIn et Facebook est traitée par Supabase Auth, l'app ne reçoit que la session Supabase.*	Non applicable
V10.5.3	2	Vérifiez que le client rejette les tentatives d'un serveur d'autorisation malveillant d'usurper l'identité d'un autre serveur d'autorisation via ses métadonnées. Le client doit rejeter les métadonnées du serveur d'autorisation si l'URL de l'émetteur figurant dans ces métadonnées ne correspond pas exactement à l'URL d'émetteur préconfigurée attendue par le client. *Opti' n'est pas partie utilisatrice OIDC : la connexion par LinkedIn et Facebook est traitée par Supabase Auth, l'app ne reçoit que la session Supabase.*	Non applicable
V10.5.4	2	Vérifiez que le client valide que le jeton d'identification est destiné à être utilisé pour ce client (audience) en vérifiant que la déclaration « aud » du jeton est égale à la valeur « client_id » pour le client. *Opti' n'est pas partie utilisatrice OIDC : la connexion par LinkedIn et Facebook est traitée par Supabase Auth, l'app ne reçoit que la session Supabase.*	Non applicable
V10.5.5	2	Vérifiez que, lors de l'utilisation de la déconnexion du back-channel OIDC, la partie utilisatrice atténue les risques de déni de service liés à la déconnexion forcée et à la confusion entre JWT dans le flux de déconnexion. Le client doit vérifier que le jeton de déconnexion est correctement typé avec la valeur « logout+jwt », qu'il contient la déclaration « event » avec le nom de membre correct et qu'il ne contient pas de déclaration « nonce ». Il est également recommandé d'utiliser une expiration courte (par exemple, 2 minutes). *Opti' n'est pas partie utilisatrice OIDC : la connexion par LinkedIn et Facebook est traitée par Supabase Auth, l'app ne reçoit que la session Supabase.*	Non applicable
V10.6.1	2	Vérifiez que le fournisseur OpenID n'autorise que les valeurs « code », « ciba », « id_token » ou « id_token code » pour le mode de réponse. Notez que « code » est préférable à « id_token code » (flux hybride OIDC) et que « token » (tout flux implicite) ne doit pas être utilisé. *Opti' n'est pas fournisseur OpenID.*	Non applicable
V10.6.2	2	Vérifiez que le fournisseur OpenID atténue les risques de déni de service liés à la déconnexion forcée. Pour ce faire, obtenez une confirmation explicite de l'utilisateur final ou, le cas échéant, validez les paramètres de la requête de déconnexion (initiée par la partie utilisatrice), comme « id_token_hint ». *Idem.*	Non applicable
V10.7.1	2	Vérifiez que le serveur d'autorisation garantit le consentement de l'utilisateur à chaque demande d'autorisation. Si l'identité du client ne peut être garantie, le serveur d'autorisation doit toujours demander explicitement le consentement de l'utilisateur. *Opti' n'est pas serveur d'autorisation (Supabase Auth, Google et Microsoft le sont).*	Non applicable
V10.7.2	2	Vérifiez que lorsque le serveur d'autorisation demande le consentement de l'utilisateur, il fournit des informations claires et suffisantes sur ce qui est consenti. Le cas échéant, ces informations doivent inclure la nature des autorisations demandées (généralement en fonction de la portée, du serveur de ressources et des détails d'autorisation RAR), l'identité de l'application autorisée et la durée de vie de ces autorisations. *Opti' n'est pas serveur d'autorisation (Supabase Auth, Google et Microsoft le sont).*	Non applicable

	Niv.	Texte	Statut
V10.7.3	2	Vérifiez que l'utilisateur peut consulter, modifier et révoquer les consentements qu'il a accordés via le serveur d'autorisation. *Opti' n'est pas serveur d'autorisation (Supabase Auth, Google et Microsoft le sont).*	Non applicable

V11 · Cryptographie

	Niv.	Texte	Statut
V11.1.1	2	Vérifiez qu'il existe une politique documentée pour la gestion des clés cryptographiques et un cycle de vie des clés cryptographiques qui suit une norme de gestion des clés telle que NIST SP 800-57. Cela devrait inclure la garantie que les clés ne sont pas sur-partagées (par exemple, avec plus de deux entités pour les secrets partagés et plus d'une entité pour les clés privées). *Politique de gestion des clés écrite (inventaire, versions, remplacement) ; quelques éléments de forme restent à ajouter.*	Partiel
V11.1.2	2	Vérifiez qu'un inventaire cryptographique est réalisé, maintenu et régulièrement mis à jour, et qu'il inclut toutes les clés, algorithmes et certificats cryptographiques utilisés par l'application. Il doit également documenter les emplacements du système où les clés peuvent ou non être utilisées, ainsi que les types de données qui peuvent ou non être protégées par ces clés.	Conforme
V11.2.1	2	Vérifiez que les implémentations validées par l'industrie (y compris les bibliothèques et les implémentations accélérées par le matériel) sont utilisées pour les opérations cryptographiques.	Conforme
V11.2.2	2	Vérifiez que l'application est conçue avec une agilité cryptographique, de sorte que les nombres aléatoires, le chiffrement authentifié, le MAC ou les algorithmes de hachage, les longueurs de clés, les tours, les chiffrements et les modes puissent être reconfigurés, mis à niveau ou échangés à tout moment, afin de se protéger contre les failles cryptographiques. De même, il doit être possible de remplacer les clés et les mots de passe, ainsi que de rechiffrer les données. Cela permettra des mises à niveau transparentes vers la cryptographie post-quantique (PQC), une fois que des implémentations hautement sécurisées de schémas ou de normes PQC approuvés seront largement disponibles. *Le chiffrement porte un numéro de version de clé, ce qui prépare un remplacement ; le rechiffrement n'est pas encore outillé.*	Partiel
V11.2.3	2	Vérifiez que toutes les primitives cryptographiques utilisent un minimum de 128 bits de sécurité en fonction de l'algorithme, de la taille de la clé et de la configuration. Par exemple, une clé ECC de 256 bits offre environ 128 bits de sécurité, tandis que RSA nécessite une clé de 3072 bits pour atteindre 128 bits de sécurité.	Conforme
V11.3.1	1	Vérifiez que les modes de bloc non sécurisés (par exemple, ECB) et les schémas de remplissage faibles (par exemple, PKCS#1 v1.5) ne sont pas utilisés.	Conforme
V11.3.2	1	Vérifiez que seuls les chiffrements et modes approuvés tels que AES avec GCM sont utilisés.	Conforme
V11.3.3	2	Vérifiez que les données chiffrées sont protégées contre toute modification non autorisée, de préférence en utilisant une méthode de chiffrement authentifiée approuvée ou en combinant une méthode de chiffrement approuvée avec un algorithme MAC approuvé.	Conforme
V11.4.1	1	Vérifiez que seules les fonctions de hachage approuvées sont utilisées pour les cas d'utilisation cryptographiques généraux, notamment les signatures numériques, HMAC, KDF et la génération de bits aléatoires. Les fonctions de hachage non autorisées, telles que MD5, ne doivent pas être utilisées à des fins cryptographiques.	Conforme
V11.4.2	2	Vérifiez que les mots de passe sont stockés à l'aide d'une fonction de dérivation de clés approuvée et gourmande en ressources de calcul (également appelée « fonction de hachage de mots de passe »), dont les paramètres sont configurés conformément aux directives en vigueur. Ces paramètres doivent équilibrer sécurité et performances afin de rendre les attaques par force brute suffisamment difficiles pour le niveau de sécurité requis.	Conforme
V11.4.3	2	Vérifiez que les fonctions de hachage utilisées dans les signatures numériques, dans le cadre de l'authentification ou de l'intégrité des données, sont résistantes aux collisions et possèdent des longueurs de bits appropriées. Si la résistance aux collisions est requise, la longueur de sortie doit être d'au moins 256 bits. Si seule la résistance aux attaques de seconde pré-image est requise, la longueur de sortie doit être d'au moins 128 bits.	Conforme

	Niv.	Texte	Statut
V11.4.4	2	Vérifiez que l'application utilise des fonctions de dérivation de clés approuvées avec des paramètres d'extension de clés lors de la dérivation de clés secrètes à partir de mots de passe. Les paramètres utilisés doivent concilier sécurité et performances afin d'empêcher les attaques par force brute de compromettre la clé cryptographique obtenue.	Conforme
V11.5.1	2	Vérifiez que tous les nombres et chaînes aléatoires destinés à être non devinables doivent être générés à l'aide d'un générateur de nombres pseudo-aléatoires cryptographiquement sécurisé (CSPRNG) et posséder au moins 128 bits d'entropie. Notez que les UUID ne respectent pas cette condition.	Conforme
V11.6.1	2	Vérifier que seuls des algorithmes cryptographiques et des modes opératoires approuvés sont utilisés pour la génération et l'amorçage des clés, ainsi que pour la génération et la vérification des signatures numériques. Les algorithmes de génération de clés ne doivent pas générer de clés non sécurisées et vulnérables aux attaques connues, par exemple les clés RSA vulnérables à la factorisation de Fermat.	Conforme

V12 · Communication sécurisée

	Niv.	Texte	Statut
V12.1.1	1	Vérifiez que seules les dernières versions recommandées du protocole TLS sont activées, telles que TLS 1.2 et TLS 1.3. La dernière version du protocole TLS doit être privilégiée.	Conforme
V12.1.2	2	Vérifiez que seules les suites de chiffrement recommandées sont activées, les suites de chiffrement les plus puissantes étant définies comme préférées. Les applications L3 doivent uniquement prendre en charge les suites de chiffrement assurant la confidentialité persistante (forward secrecy).	Conforme
V12.1.3	2	Vérifiez que l'application valide que les certificats clients mTLS sont approuvés avant d'utiliser l'identité du certificat pour l'authentification ou l'autorisation. *Aucune authentification par certificat client.*	Non applicable
V12.2.1	1	Vérifiez que TLS est utilisé pour toute connectivité entre un client et des services externes basés sur HTTP, et ne recourt pas à des communications non sécurisées ou non chiffrées.	Conforme
V12.2.2	1	Vérifiez que les services externes utilisent des certificats TLS publiquement approuvés.	Conforme
V12.3.1	2	Vérifiez qu'un protocole chiffré tel que TLS est utilisé pour toutes les connexions entrantes et sortantes vers et depuis l'application, y compris les systèmes de surveillance, les outils de gestion, l'accès à distance et SSH, les intergiciels, les bases de données, les mainframes, les systèmes partenaires ou les API externes. Le serveur ne doit pas recourir à des protocoles non sécurisés ou non chiffrés.	Conforme
V12.3.2	2	Vérifiez que les clients TLS valident les certificats reçus avant de communiquer avec un serveur TLS.	Conforme
V12.3.3	2	Vérifiez que TLS ou un autre mécanisme de chiffrement de transport approprié est utilisé pour toute connectivité entre les services internes basés sur HTTP au sein de l'application et ne se replie pas vers des communications non sécurisées ou non chiffrées.	Conforme
V12.3.4	2	Vérifiez que les connexions TLS entre les services internes utilisent des certificats de confiance. Lorsque des certificats générés en interne ou auto-signés sont utilisés, le service consommateur doit être configuré pour n'approuver que des autorités de certification internes spécifiques et des certificats auto-signés spécifiques.	Conforme

V13 · Configuration

	Niv.	Texte	Statut
V13.1.1	2	Vérifiez que tous les besoins de communication de l'application sont documentés. Cela doit inclure les services externes dont l'application dépend et les cas où un utilisateur final pourrait fournir un emplacement externe auquel l'application se connectera.	Conforme
V13.2.1	2	Vérifiez que les communications entre les composants de l'application backend qui ne prennent pas en charge le mécanisme de session utilisateur standard de l'application, notamment les API, les intergiciels et les couches de données, sont authentifiées. L'authentification doit utiliser des comptes de service individuels, des jetons à court terme ou une authentification par certificat, et non des identifiants immuables tels que des mots de passe, des clés API ou des comptes partagés avec accès privilégié.	Conforme

	Niv.	Texte	Statut
V13.2.2	2	Vérifiez que les communications entre les composants de l'application backend, y compris les services locaux ou du système d'exploitation, les API, les intergiciels et les couches de données, sont effectuées avec des comptes dotés des privilèges les moins nécessaires. *L'API utilise une clé de service qui contourne les règles de la base ; elle porte donc elle-même le contrôle de chaque route. Pas de rôle de base à privilèges réduits.*	Partiel
V13.2.3	2	Vérifiez que si des informations d'identification doivent être utilisées pour l'authentification du service, les informations d'identification utilisées par le consommateur ne sont pas des informations d'identification par défaut (par exemple, root/root ou admin/admin).	Conforme
V13.2.4	2	Vérifiez qu'une liste d'autorisations est utilisée pour définir les ressources ou systèmes externes avec lesquels l'application est autorisée à communiquer (par exemple, pour les requêtes sortantes, les chargements de données ou l'accès aux fichiers). Cette liste d'autorisation peut être implémentée au niveau de la couche applicative, du serveur web, du pare-feu ou d'une combinaison de différentes couches. *Les fournisseurs appelés sont fixes ; deux sorties suivent une adresse donnée par l'utilisateur (lecture d'une page web, serveur Kobo), protégées contre les adresses privées.*	Partiel
V13.2.5	2	Vérifiez que le serveur Web ou d'application est configuré avec une liste autorisée de ressources ou de systèmes vers lesquels le serveur peut envoyer des requêtes ou charger des données ou des fichiers. *Même constat ; l'hébergeur ne propose pas de filtrage des sorties réseau sur l'offre utilisée.*	Partiel
V13.3.1	2	Vérifiez qu'une solution de gestion des secrets, telle qu'un coffre-fort de clés, est utilisée pour créer, stocker, contrôler l'accès et détruire en toute sécurité les secrets backend. Ceux-ci peuvent inclure des mots de passe, du matériel de clé, des intégrations avec des bases de données et des systèmes tiers, des clés et des graines pour des jetons temporels, d'autres secrets internes et des clés API. Les secrets ne doivent pas être inclus dans le code source de l'application ni dans les artefacts de build. Pour une application L3, cela doit impliquer une solution matérielle telle qu'un HSM. *Secrets dans les variables de l'hébergeur et dans le coffre de la base, jamais dans le code ; pas de coffre unique.*	Partiel
V13.3.2	2	Vérifiez que l'accès aux ressources secrètes respecte le principe du moindre privilège. *Clé de paiement restreinte ; la clé de service de la base donne tous les droits et sert à toute l'API.*	Partiel
V13.4.1	1	Vérifiez que l'application est déployée soit sans aucune métadonnée de contrôle de source, y compris les dossiers .git ou .svn, soit de manière à ce que ces dossiers soient inaccessibles à la fois en externe et à l'application elle-même.	Conforme
V13.4.2	2	Vérifiez que les modes de débogage sont désactivés pour tous les composants dans les environnements de production afin d'éviter l'exposition des fonctionnalités de débogage et la fuite d'informations.	Conforme
V13.4.3	2	Vérifiez que les serveurs Web n'exposent pas les listes de répertoires aux clients, sauf si cela est explicitement prévu.	Conforme
V13.4.4	2	Vérifiez que l'utilisation de la méthode HTTP TRACE n'est pas prise en charge dans les environnements de production, afin d'éviter toute fuite d'informations potentielle.	Conforme
V13.4.5	2	Vérifiez que la documentation (comme pour les API internes) et les endpoints de surveillance ne sont pas exposés, sauf si cela est explicitement prévu.	Conforme

V14 · Protection des données

	Niv.	Texte	Statut
V14.1.1	2	Vérifiez que toutes les données sensibles créées et traitées par l'application ont été identifiées et classées selon leur niveau de protection. Cela inclut les données uniquement codées et donc facilement déchiffrables, telles que les chaînes Base64 ou la charge utile en texte clair d'un JWT. Les niveaux de protection doivent tenir compte des réglementations et normes de protection des données et de confidentialité auxquelles l'application est tenue de se conformer.	Conforme

	Niv.	Texte	Statut
V14.1.2	2	Vérifier que tous les niveaux de protection des données sensibles sont assortis d'un ensemble documenté d'exigences de protection. Cela doit inclure (sans s'y limiter) les exigences relatives au chiffrement général, à la vérification de l'intégrité, à la conservation, à la journalisation des données, aux contrôles d'accès aux données sensibles dans les journaux, au chiffrement au niveau de la base de données, aux technologies de confidentialité et de renforcement de la confidentialité à utiliser, ainsi qu'aux autres exigences de confidentialité.	Conforme
V14.2.1	1	Vérifiez que les données sensibles sont uniquement envoyées au serveur dans les champs de corps ou d'en-tête du message HTTP, et que l'URL et la chaîne de requête ne contiennent pas d'informations sensibles, telles qu'une clé API ou un jeton de session. *Aucun jeton de session dans les adresses. Y restent, par nature : les liens signés des e-mails et le jeton d'un lien de saisie.*	Partiel
V14.2.2	2	Vérifiez que l'application empêche la mise en cache des données sensibles dans les composants du serveur, tels que les équilibreurs de charge et les caches d'application, ou garantit que les données sont purgées en toute sécurité après utilisation.	Conforme
V14.2.3	2	Vérifiez que les données sensibles définies ne sont pas envoyées à des parties non fiables (par exemple, des trackers d'utilisateurs) pour empêcher la collecte indésirable de données en dehors du contrôle de l'application. *Aucun traceur tiers dans l'application, la page de saisie ni le site ; le complément Excel charge un outil de mesure d'audience.*	Partiel
V14.2.4	2	Vérifiez que les contrôles autour des données sensibles liés au chiffrement, à la vérification de l'intégrité, à la conservation, à la manière dont les données doivent être enregistrées, aux contrôles d'accès autour des données sensibles dans les journaux, à la confidentialité et aux technologies d'amélioration de la confidentialité, sont mis en œuvre comme défini dans la documentation pour le niveau de protection des données spécifiques.	Conforme
V14.3.1	1	Vérifiez que les données authentifiées sont effacées du stockage client, comme le DOM du navigateur, après la fin du client ou de la session. Le champ d'en-tête de réponse HTTP « Clear-Site-Data » peut être utile, mais le côté client devrait également pouvoir effectuer la correction si la connexion au serveur n'est pas disponible à la fin de la session.	Conforme
V14.3.2	2	Vérifiez que l'application définit suffisamment de champs d'en-tête de réponse HTTP anti-caching (c'est-à-dire Cache-Control : no-store) afin que les données sensibles ne soient pas mises en cache dans les navigateurs.	Conforme
V14.3.3	2	Vérifiez que les données stockées dans le stockage du navigateur (telles que localStorage, sessionStorage, IndexedDB ou les cookies) ne contiennent pas de données sensibles, à l'exception des jetons de session. *L'application garde des données dans le navigateur pour fonctionner hors connexion ; elles sont effacées à la déconnexion, sauf ce que la personne choisit de garder.*	Non conforme

V15 · Développement et architecture sécurisés

	Niv.	Texte	Statut
V15.1.1	1	Vérifiez que la documentation de l'application définit les délais de correction basés sur les risques pour les versions de composants tiers présentant des vulnérabilités et pour la mise à jour des bibliothèques en général, afin de minimiser les risques liés à ces composants.	Conforme
V15.1.2	2	Vérifiez qu'un catalogue d'inventaire, tel qu'une nomenclature logicielle (SBOM), est conservé pour toutes les bibliothèques tierces utilisées, y compris en vérifiant que les composants proviennent de référentiels prédéfinis, fiables et continuellement maintenus.	Conforme
V15.1.3	2	Vérifiez que la documentation de l'application identifie les fonctionnalités consommatrices en temps ou gourmandes en ressources. Elle doit notamment indiquer comment prévenir une perte de disponibilité due à une utilisation excessive de ces fonctionnalités et éviter que la génération d'une réponse ne prenne plus de temps que le délai d'expiration du consommateur. Les mesures de protection potentielles peuvent inclure le traitement asynchrone, l'utilisation de files d'attente et la limitation des processus parallèles par utilisateur et par application.	Conforme

	Niv.	Texte	Statut
V15.2.1	1	Vérifiez que l'application contient uniquement des composants qui n'ont pas dépassé les délais de mise à jour et de correction documentés. *Dépendances mises à jour, aucune faille connue atteignable en production ; quelques failles résiduelles, non atteignables, sont suivies.*	Partiel
V15.2.2	2	Vérifiez que l'application a mis en œuvre des défenses contre la perte de disponibilité due à des fonctionnalités qui prennent du temps ou qui nécessitent des ressources, sur la base des décisions et stratégies de sécurité documentées à cet effet. *Plafonds de crédits, de requêtes et de ressources sur les fonctions coûteuses ; pas de limite générale de concurrence.*	Partiel
V15.2.3	2	Vérifiez que l'environnement de production inclut uniquement les fonctionnalités nécessaires au fonctionnement de l'application et n'expose pas de fonctionnalités superflues telles que du code de test, des exemples d'extraits et des fonctionnalités de développement. *Les routes d'essai ne sont pas exposées, sauf une, plafonnée en débit.*	Partiel
V15.3.1	1	Vérifiez que l'application ne renvoie que le sous-ensemble requis de champs d'un objet de données. Par exemple, elle ne doit pas renvoyer un objet de données entier, car certains champs individuels ne doivent pas être accessibles aux utilisateurs.	Conforme
V15.3.2	2	Vérifiez que lorsque le backend de l'application effectue des appels vers des URL externes, il est configuré pour ne pas suivre les redirections, sauf s'il s'agit d'une fonctionnalité prévue.	Conforme
V15.3.3	2	Vérifiez que l'application dispose de contre-mesures pour se protéger contre les attaques d'affectation de masse en limitant les champs autorisés par contrôleur et action, par exemple, il n'est pas possible d'insérer ou de mettre à jour une valeur de champ lorsqu'elle n'était pas destinée à faire partie de cette action.	Conforme
V15.3.4	2	Vérifiez que tous les composants proxy et middleware transfèrent correctement l'adresse IP d'origine de l'utilisateur à l'aide de champs de données fiables qui ne peuvent pas être manipulés par l'utilisateur final, et que l'application et le serveur Web utilisent cette valeur correcte pour la journalisation et les décisions de sécurité telles que la limitation du débit, en tenant compte du fait que même l'adresse IP d'origine peut ne pas être fiable en raison d'adresses IP dynamiques, de VPN ou de pare-feu d'entreprise.	Conforme
V15.3.5	2	Vérifiez que l'application garantit explicitement que les variables sont du type correct et effectue des opérations d'égalité et de comparaison strictes. Cela permet d'éviter les vulnérabilités liées à la confusion de types, causées par des hypothèses du code de l'application sur le type d'une variable. *Identifiants validés par format et chaînes forcées ; les comparaisons strictes ne sont pas systématiques dans tout le code.*	Partiel
V15.3.6	2	Vérifiez que le code JavaScript est écrit de manière à éviter la pollution du prototype, par exemple en utilisant Set() ou Map() au lieu de littéraux d'objet. *Aucune fusion d'objets reçus relevée ; la bibliothèque de lecture Excel concernée par cette faille est corrigée. Revue non exhaustive.*	Partiel
V15.3.7	2	Vérifiez que l'application dispose de défenses contre les attaques de pollution des paramètres HTTP, en particulier si le Framework d'application ne fait aucune distinction quant à la source des paramètres de requête (chaîne de requête, paramètres de corps, cookies ou champs d'en-tête). *Les paramètres d'adresse sont forcés en chaînes sur les routes lues ; pas de règle générale.*	Partiel

V16 · Journalisation de sécurité et gestion des erreurs

	Niv.	Texte	Statut
V16.1.1	2	Vérifiez qu'il existe un inventaire documentant la journalisation effectuée à chaque couche de la pile technologique de l'application, les événements enregistrés, les formats de journal, l'endroit où cette journalisation est stockée, la manière dont elle est utilisée, la manière dont l'accès à celle-ci est contrôlé et la durée de conservation des journaux.	Conforme
V16.2.1	2	Vérifiez que chaque entrée de journal inclut les métadonnées nécessaires (telles que quand, où, qui, quoi) qui permettraient une enquête détaillée sur la chronologie lorsqu'un événement se produit.	Conforme
V16.2.2	2	Vérifiez que les sources de temps de tous les composants de journalisation sont synchronisées et que les horodatages des métadonnées des événements de sécurité utilisent le temps UTC ou incluent un décalage horaire explicite. L'UTC est recommandé pour garantir la cohérence entre les systèmes distribués et éviter toute confusion lors du passage à l'heure d'été.	Conforme

	Niv.	Texte	Statut
V16.2.3	2	Vérifiez que l'application stocke ou diffuse uniquement les journaux vers les fichiers et services documentés dans l'inventaire des journaux.	Conforme
V16.2.4	2	Vérifiez que les journaux peuvent être lus et corrélés par le processeur de journaux utilisé, de préférence en utilisant un format de journalisation commun.	Conforme
V16.2.5	2	Vérifiez que l'application applique la journalisation en fonction du niveau de protection des données lors de la journalisation de données sensibles. Par exemple, certaines données, comme les identifiants ou les informations de paiement, peuvent être interdites. D'autres données, comme les jetons de session, ne peuvent être enregistrées que par hachage ou masquage, en totalité ou en partie.	Conforme
V16.3.1	2	Vérifiez que toutes les opérations d'authentification sont enregistrées, y compris les tentatives réussies et infructueuses. Des métadonnées supplémentaires, telles que le type d'authentification ou les facteurs utilisés, doivent également être collectées.	Conforme
V16.3.2	2	Vérifier que les tentatives d'autorisation infructueuses sont logguées. Pour le niveau 3, cela doit inclure la journalisation de toutes les décisions d'autorisation, y compris lors de l'accès à des données sensibles (sans journalisation des données sensibles elles-mêmes). *Les refus d'identité sont journalisés par l'API ; les refus des règles de la base ne le sont que dans les journaux de l'hébergeur.*	Partiel
V16.3.3	2	Vérifiez que l'application enregistre les événements de sécurité définis dans la documentation et enregistre également les tentatives de contournement des contrôles de sécurité, tels que la validation des entrées, la logique métier et l'anti-automatisation.	Conforme
V16.3.4	2	Vérifiez que l'application enregistre les erreurs inattendues et les échecs de contrôle de sécurité tels que les échecs TLS du backend.	Conforme
V16.4.1	2	Vérifiez que tous les composants de journalisation codent correctement les données pour empêcher l'injection de journaux.	Conforme
V16.4.2	2	Vérifiez que les journaux sont protégés contre tout accès non autorisé et ne peuvent pas être modifiés.	Conforme
V16.4.3	2	Vérifiez que les journaux sont transmis de manière sécurisée à un système logique distinct pour analyse, détection, alerte et remontée des informations. L'objectif est de garantir qu'en cas de violation de l'application, les journaux ne seront pas compromis. *Pas de système de journaux distinct pour l'analyse et l'alerte ; les journaux restent chez chaque hébergeur.*	Non conforme
V16.5.1	2	Vérifiez qu'un message générique est renvoyé au consommateur lorsqu'une erreur inattendue ou sensible à la sécurité se produit, garantissant ainsi l'absence d'exposition de données système internes sensibles telles que les traces de pile, les requêtes, les clés secrètes et les jetons.	Conforme
V16.5.2	2	Vérifiez que l'application continue de fonctionner en toute sécurité lorsque l'accès aux ressources externes échoue, par exemple, en utilisant des modèles tels que des disjoncteurs ou une dégradation progressive.	Conforme
V16.5.3	2	Vérifiez que l'application échoue proprement et sécurisée, y compris lorsqu'une exception se produit, en évitant les accès en cas d'erreur telles que le traitement d'une transaction malgré les erreurs résultant de la logique de validation.	Conforme

V17 · WebRTC

	Niv.	Texte	Statut
V17.1.1	2	Vérifiez que le service TURN (Traversal Using Relays around NAT) autorise uniquement l'accès aux adresses IP non réservées à des fins spécifiques (par exemple, réseaux internes, diffusion, bouclage). Notez que cela s'applique aux adresses IPv4 et IPv6. *Aucun WebRTC : l'enregistrement audio des focus groups passe par MediaRecorder, sans serveur multimédia.*	Non applicable
V17.2.1	2	Vérifiez que la clé du certificat Datagram Transport Layer Security (DTLS) est gérée et protégée conformément à la politique documentée de gestion des clés cryptographiques. *Aucun WebRTC : l'enregistrement audio des focus groups passe par MediaRecorder, sans serveur multimédia.*	Non applicable

	Niv.	Texte	Statut
V17.2.2	2	Vérifiez que le serveur multimédia est configuré pour utiliser et prendre en charge les suites de chiffrement DTLS (Datagram Transport Layer Security) approuvées et un profil de protection sécurisé pour l'extension DTLS pour l'établissement de clés pour le protocole de transport en temps réel sécurisé (DTLS-SRTP). *Aucun WebRTC : l'enregistrement audio des focus groups passe par MediaRecorder, sans serveur multimédia.*	Non applicable
V17.2.3	2	Vérifiez que l'authentification SRTP (Secure Real-time Transport Protocol) est vérifiée sur le serveur multimédia pour empêcher les attaques par injection RTP (Real-time Transport Protocol) d'entraîner une condition de déni de service ou l'insertion de médias audio ou vidéo dans les flux multimédias. *Aucun WebRTC : l'enregistrement audio des focus groups passe par MediaRecorder, sans serveur multimédia.*	Non applicable
V17.2.4	2	Vérifiez que le serveur multimédia est en mesure de continuer à traiter le trafic multimédia entrant lorsqu'il rencontre des paquets SRTP (Secure Real-time Transport Protocol) mal formés. *Aucun WebRTC : l'enregistrement audio des focus groups passe par MediaRecorder, sans serveur multimédia.*	Non applicable
V17.3.1	2	Vérifiez que le serveur de signalisation est capable de continuer à traiter les messages de signalisation entrants légitimes lors d'une attaque par saturation. Cela peut être réalisé en implémentant une limitation de débit au niveau de la signalisation. *Aucun WebRTC : l'enregistrement audio des focus groups passe par MediaRecorder, sans serveur multimédia.*	Non applicable
V17.3.2	2	Vérifiez que le serveur de signalisation est capable de continuer à traiter les messages de signalisation légitimes en cas de message mal formé susceptible de provoquer un déni de service. Cela peut inclure la validation des entrées, la gestion sécurisée des dépassements d'entiers, la prévention des dépassements de tampon et l'utilisation d'autres techniques robustes de gestion des erreurs. *Aucun WebRTC : l'enregistrement audio des focus groups passe par MediaRecorder, sans serveur multimédia.*	Non applicable

B Annexe : OWASP Top 10 des applications à base de modèles de langage (2025)

Les dix risques propres aux applications qui utilisent l'IA générative, tels que les liste l'OWASP (édition 2025), et ce qu'Opti' fait pour chacun. Périmètre : OptiBot, Opti Gemba (questionnaires, termes de référence, rapports, « Demande à tes données »), Opti Academy, génération d'images, OptIA. Évaluation interne, par lecture du code et essais.

Risques	Conformes	Maîtrisés, risque résiduel accepté	Partiels	Non conformes
10	9	1	0	0

	Ce qu'Opti' fait	Statut
LLM01 **Injection d'instructions**	Les droits, les crédits et l'accès aux données sont décidés par le serveur et la base, jamais par le modèle. Le modèle n'a que des outils de lecture : un texte piégé (document importé, page web) peut orienter une réponse, mais ne peut ni écrire, ni supprimer, ni faire sortir de données. Une adresse web n'est lue que si l'utilisateur l'a donnée ou si la recherche l'a rendue. *Risque résiduel commun à tous les assistants de ce type : une réponse orientée reste possible ; elle est relue par l'utilisateur avant tout usage.*	Maîtrisé
LLM02 **Divulgation d'informations sensibles**	La recherche documentaire ne porte que sur les documents du compte (ou partagés avec lui) ; les tables des extraits sont fermées au navigateur ; les conversations sont chiffrées ; aucun contenu de conversation n'est journalisé ; les réponses n'affichent pas d'images distantes, canal classique de fuite.	Conforme
LLM03 **Chaîne d'approvisionnement**	Mistral et OpenAI par leurs API officielles. OptIA : version du moteur figée, fichier du modèle vérifié par son empreinte avant usage.	Conforme
LLM04 **Empoisonnement des données ou du modèle**	Aucun entraînement ni affinage. La base de connaissances commune n'est alimentée que par l'éditeur ; les documents d'un utilisateur ne servent qu'à lui et à ceux avec qui il les partage.	Conforme
LLM05 **Traitement inadapté des sorties**	Le texte du modèle est échappé avant affichage ; les liens sont limités à http et https ; le HTML enregistré est nettoyé ; le code écrit par le modèle pour un calcul s'exécute dans un bac à sable isolé (sans réseau ni fichiers, temps et mémoire bornés) ; les formules des questionnaires sont évaluées par un analyseur, jamais exécutées.	Conforme
LLM06 **Autonomie excessive**	Tous les outils du modèle sont en lecture (recherche, lecture d'une page, bibliothèque du compte, calcul) ; le nombre d'appels d'outils est borné par réponse. Aucune écriture, aucun envoi, aucun paiement, aucune suppression : toute génération est déclenchée et relue par l'utilisateur.	Conforme
LLM07 **Fuite des instructions système**	Les instructions des modèles ne contiennent ni clé, ni secret, ni donnée d'un autre compte. Aucune règle de sécurité ne repose sur elles : leur divulgation n'ouvrirait rien.	Conforme
LLM08 **Faiblesses des vecteurs et plongements**	Les extraits vectorisés sont en base, dans des tables fermées au navigateur ; la recherche reçoit la liste explicite des documents autorisés pour le compte, et une liste vide l'arrête.	Conforme
LLM09 **Désinformation**	Les chiffres d'un rapport sont calculés sur les réponses puis rapprochés automatiquement du texte ; les calculs sur tableaux sont exécutés et contrôlés ; les sources sont citées ; tout document produit reste modifiable et doit être relu avant diffusion. La méthode du générateur de questionnaires et celle du rapport sont publiées, avec une fiche de transparence SAFE AI.	Conforme
LLM10 **Consommation sans limite**	Crédits par compte vérifiés avant chaque appel ; plafonds par compte, par adresse réseau et globaux sur les routes publiques ; OptIA réservée aux formules qui l'incluent ; nombre d'appels d'outils borné.	Conforme

Référentiel : OWASP Top 10 for LLM Applications 2025, OWASP Foundation, genai.owasp.org.