Roadmap SOC 2 Type 1 — Scope

Programme de certification — partenaire d'automatisation : Vanta · version 2026.04.28-v1 · 2026-04-28

Périmètre

- Trust Services Criteria : Security (CC1-CC9). Confidentiality et Availability ajoutées en Type 2.
- Système : application Scope (frontend Next.js, API serverless, base Supabase, sous-traitants ultérieurs listés au DPA).
- Auditeur indépendant : à sélectionner en M2 parmi A-LIGN, Prescient Assurance ou Insight Assurance.

M1 — Kick-off (semaine 1)

- Contrat Vanta signé. Onboarding des intégrations (GitHub, Vercel, Supabase, AWS via Supabase, Stripe, Resend).
- Politique de sécurité, plan de réponse à incident, BCP/DRP rédigés et publiés en interne.
- Inventaire des actifs et matrice des risques initialisés. Owners désignés.
- Onboarding employee/contractor checklist (background check, NDA, accès minimum) opérationnels.

M2 — Contrôles continus (semaines 4-8)

- Vanta surveille en continu MFA, gestion des accès, chiffrement, gestion des vulnérabilités, formation sécurité.
- Pen test externe planifié (Cobalt ou Pentest People) — rapport remis à l'auditeur.
- Sentry remplacé par GlitchTip auto-hébergé UE pour fermer la dépendance Cloud Act.
- Sélection définitive de l'auditeur indépendant. Lettre d'engagement signée.

M3 — Scan de pré-audit complet (semaine 12)

- Vanta indique 100 % de contrôles verts. Toutes les politiques sont approuvées et signées.
- Badge « SOC 2 Type 1 in progress » affichable publiquement.
- Premier sample Type 1 fourni à l'auditeur (point-in-time evidence).

M4-M5 — Audit (semaines 16-20)

- Auditeur réalise les tests de design des contrôles.
- Itérations sur les findings éventuels (objectif zéro qualified opinion).
- Plan de remédiation pour les findings non bloquants — délai 30 jours.

M6 — Attestation Type 1 délivrée (semaine 24)

- Rapport SOC 2 Type 1 reçu, signé et publiable sous accord de confidentialité.
- Page /trust mise à jour : statut « Disponible · 2026-09-28 ».
- Lancement Type 2 (audit de fonctionnement sur 3 à 12 mois) — cible attestation Type 2 M15-M18.

Budget

Vanta : 8 à 12 k€ / an (tier startup, négocié).

Pen test : 3 à 5 k€ ponctuel (M2).

Auditeur indépendant : 5 à 8 k€ pour le rapport Type 1.

Total Année 1 : 16 à 25 k€, à comparer aux >300 k€ de pipeline débloqués (cf. STRATEGY-2026-04-28 §5.1).

Suivi public

L'avancement est publié mensuellement sur https://getscope.dev/trust et notifié par email aux clients abonnés. Les clients Enterprise reçoivent en plus un point de situation trimestriel avec leur Customer Success Manager.