الأمان

موجز الأمان

ما تفعله المنصة لحماية منشأتك، مذكوراً من الكود واختباراته.

التحكم بالوصول

- مفاتيح API مجزّأة لكل منشأة؛ ومفتاح الإدارة للمشغّلين فقط.
- دخول الأعضاء بكلمات مرور scrypt، وجلسات محفوظة كبصمة SHA-256 بانتهاء خمول وانتهاء مطلق.
- الأدوار: مالك، مدير، موظف، مسؤول فوترة. الصلاحيات ترفض افتراضياً على كل مسار.
- تحقق بخطوتين (TOTP) مع رموز استرداد لمرة واحدة.

حماية الأسرار

- رموز المزوّدين وأسرار التحقق بخطوتين مشفّرة بـ Fernet بمفتاح خارج قاعدة البيانات.
- لا يُرجع أي API سراً أو رمزاً أو نصاً مشفّراً؛ والسجلات تحجب الرموز.
- يرفض وضع الإنتاج الإقلاع بلا أسرار التحكم بالوصول.

العزل بين المنشآت

- التوجيه يطابق زوج (الحساب، صندوق الوارد) بالضبط؛ وكل ملتبس يُحجر.
- مصادر المعرفة وسجلات التوجيه والتذاكر محصورة بالمنشأة.
- كل تغيير حساس يُكتب في سجل التدقيق بلا أسرار.

ضمانات التوصيل

- كل Webhook يُخزَّن قبل معالجته؛ والإخفاقات قابلة لإعادة المحاولة.
- لا يمكن لرد ذكي متأخر أن يتجاوز الموظف: تُفحص الملكية قبل كل إرسال.
- أخطاء المزوّد لا تُنتج نصاً للعميل أبداً؛ بل تحويلاً مع ملاحظة.

التعامل مع البيانات

- المحادثات في صندوق وارد تشات وورك الخاص بك؛ والجسر لا يحتفظ بنسخة ثانية.
- بيانات طلبات سلة وزد تُخزَّن مؤقتاً بلا اسم العميل أو عنوانه أو جواله أو بريده.
- الروابط الصادرة يجب أن تكون https وعلى عناوين عامة (حماية SSRF).

التشغيل

- استضافة ذاتية: Docker Compose و PostgreSQL و Redis و Caddy بشهادات TLS تلقائية.
- نقطتا فحص للحياة والجاهزية؛ ومعرّف طلب على كل استجابة.
- بوابة فحص واحدة: أكثر من 900 اختبار تشمل طبقة قاعدة البيانات، قبل أي إصدار.

حدود معلنة

- لا يُتحقق من البريد عند التسجيل حتى الآن؛ استخدم وضع الرمز أو الإغلاق على الخوادم العامة.
- ZATCA: بيانات رمز QR للمرحلة الأولى فقط؛ وليست ادعاء امتثال.
- الطبقة الدلالية لم تُجرَّب بعد على مزوّد تضمينات حقيقي.