ROL BAZLI REHBER 361

CISO / GÜVENLİK & UYUM İÇİN

CISO için 361 Rehberi

Gölge AI ve veri sızıntısını mimari düzeyde kapatın: fail-closed RLS, guardrail, on-prem, denetim.

4	Fail-closed	On-prem
guardrail detektörü	RLS varsayılanı	veri çıkmaz

Gölge AI ve veri sızıntısını mimari düzeyde kapatın: fail-closed RLS, guardrail, on-prem, denetim.

Rolünüzün karşılaştığı zorluklar

Gölge AI & veri sızıntısı

Çalışanlar veriyi harici sohbet araçlarına yapıştırıyor.

Yetki aşımı & halüsinasyon

Genel AI, yetkisiz veriyi özetleyebilir/uydurabilir.

KVKK/GDPR ispatı

Erişim ve değişiklik kanıtlanamıyor.

361 nasıl çözer

Zorluk	361 Yanıtı
Veri sızıntısı	On-prem yerel AI (localOnly=true) — veri makineden çıkmaz
Yetki aşımı	Fail-closed RLS: agent çağıran kullanıcının izin bağlamıyla erişir
Halüsinasyon/injection	4-detektör guardrail: PII, halüsinasyon, prompt-injection, maliyet

Zorluk	361 Yanıtı
Denetim	SHA-256 hash-chain iz + HSM/PAdES imza + MFA/SSO

Ne kazanırsınız

Gölge AI kapatıldı

On-prem localOnly ile veri makineden çıkmaz.

Yetki-sınırlı AI

Fail-closed RLS: AI, çağıran kullanıcının izin bağlamıyla erişir.

Kanıtlanabilir uyum

4-detektör guardrail + SHA-256 hash-chain denetim izi.

İlk 90 gün

1. **Risk taraması** — gölge AI
2. **RLS + guardrail** — devreye al
3. **On-prem** — localOnly
4. **Denetle** — hash-chain

CISO / Güvenlik & Uyum için tipik benimseme yolu

Neden 361?

- Fail-closed: izin yoksa erişim reddedilir
- AI = kullanıcı izniyle sınırlı, servis hesabı değil
- Sözleşmeye yazılabilir teknik garanti (localOnly)
- Tamper-evident denetim: kriptografik kanıt

SONRAKİ ADIM

CISO / Güvenlik & Uyum olarak 361'i kendi verinizde görün

2 haftalık ücretsiz POC — gerçek süreçlerinizde, sıfır risk. Kurulum yok, mevcut sisteminize dokunmadan; beğenmezseniz hiçbir şey değişmez.

Hemen başlayın

17 sağlayıcı · 52 tool · 8 kanal ailesi/44 adaptör · 200+ modül

361.com.tr · info@361.com.tr