PMS/OTA API Güvenliği & Scope/Rate Limit Planlama Şablonu (v1.0)

Asset Amacı: Bu doküman, PMS/OTA entegrasyonlarında güvenliği teknik bir standart seviyesine (Secret Management, Least Privilege, IP Allowlist) taşımak için hazırlanmıştır. Amacı, API bileşenlerini tek tabloda analiz ederek riskleri kapatmak ve olası bir sızıntı (incident) anında anahtar rotasyonu gibi prosedürleri hızla devreye almaktır.

Kim Kullanır?: Otel entegrasyon geliştiricileri, teknik liderler, BT/IT ekipleri ve B2B entegrasyon yöneticileri.

Nasıl Kullanılır? (3 Adım)

1. **Envanter Çıkarın:** Entegrasyon bileşenlerini (Web, CRM, Gateway) ve erişilen endpoint/veri gruplarını listeleyin.
2. **Kısıtları Tanımlayın:** İzinleri (Scope) minimuma indirin, IP allowlist ve rate limit profillerini oluşturun.
3. **Audit & Sprint:** Mevcut durumu skorlayın, eksikleri sprint planına dahil edin ve acil durum rotasyon prosedürünü test edin.

B) Template: Boş Şablon Alanları

1) Entegrasyon Envanteri & İzin Matrisi

(Bileşen, Sağlayıcı, Endpoint Grubu, Okuma/Yazma Yetkisi, Kritik Veri ve Sorumlu alanlarını doldurun.)

2) Secret Management & Ağ Kısıtı

- **Secret Lokasyonu:** (Secret Manager / Env Var / Diğer: ___)
- **Repo Kontrolü & Log Masking:** Secret'lar kod içinde mi? Log'larda gizleniyor mu? (E/H)
- **IP Allowlist Durumu:** Çıkış IP'leri ve VPN/Jump Host gerekliliklerini bileşen bazlı tanımlayın.

3) Rate Limit & Throttle Profilleri

- **Endpoint Grubu / Limit:** Örn: Rezervasyon API / 100 request/min.
- **Aşım Davranışı:** (429 Too Many Requests / Challenge / Block).

C) Audit Sheet (Olgunluk Skoru)

Kategori	Skor (0-5)	İlk 10 Aksiyon Listesi
Secret Management	___	1. _____
Least Privilege (Scope)	___	2. _____
IP Allowlist Kapsamı	___	3. _____
Rate Limit / Abuse	___	4. _____
Log/Audit & KVKK	___	5. _____

Incident Prosedürü (Hızlı Aksiyon)

1. **Sinyal:** Şüpheli kullanım veya yetkisiz IP erişimi tespiti.
2. **İlk Müdahale:** İlgili API Key'in anlık pasife alınması veya scope'un salt okunur (read-only) hale getirilmesi.
3. **Rotasyon:** Yeni anahtar üretimi, secret manager güncellenmesi ve eski anahtarın iptali.

Deliverables

- **Deliverables:** Entegrasyon Envanteri, Scope/Izin Matrisi, Rate Limit Profilleri, Audit Skor Tablosu ve 10 Maddelik Aksiyon Planı.