7. Stratejik Planlama ve Yönetim

Bu raporda tespit edilen "Replay (Tekrar Oynatma)" anomalisinin giderilmesi ve sürdürülebilir bir güvenlik mimarisi oluşturulması için stratejik analiz (SWOT) ve uygulama hedefleri (SMART) aşağıda detaylandırılmıştır.

7.1. SWOT Analizi (Güçlü ve Zayıf Yönler)

Sisteme **TLS Şifreleme (WSS)** ve **Message ID Kontrolü** entegrasyonu stratejisinin analizi şöyledir:

GÜÇLÜ YÖNLER (Strengths)	**ZAYIF YÖNLER (Weaknesses)**
+ Tam Gizlilik: Ağ trafiği şifrelendiği için (WSS) saldırganlar paket içeriğini göremez ve kopyalayamaz.	**- Donanım Maliyeti:** Eski nesil bazı şarj üniteleri (CPU kapasitesi düşük olanlar) şifreleme işlemini desteklemeyebilir.
+ Veri Bütünlüğü: CSMS veritabanında mükerrer ve hatalı işlem kayıtlarının oluşması engellenir.	**- Performans Gecikmesi:** Şifreleme/Çözme işlemi, haberleşme hızında milisaniyelik (latency) gecikmelere yol açabilir.
+ Standart Uyumu: Sistem, uluslararası OCPP 2.0.1 ve ISO 15118 güvenlik standartlarına tam uyumlu hale gelir.	**- Yönetim Yükü:** Yüzlerce cihazın dijital sertifikalarının (PKI) yönetimi ek operasyonel iş yükü getirir.
FIRSATLAR (Opportunities)	**TEHDİTLER (Threats)**

+ Marka İtibarı: "Güvenli Şarj Ağı" sertifikasyonu ile kurumsal filolar için tercih sebebi olunur.	**- Anahtar Yönetimi Riski:** Şifreleme anahtarlarının (Private Key) çalınması durumunda tüm koruma sistemi çökebilir.
+ Yasal Güvence: Olası dolandırıcılık davalarında, operatörün (CPO) gerekli tüm siber güvenlik önlemlerini aldığı kanıtlanabilir.	**- Fiziksel Saldırıya Yönelim:** Ağdan sızamayan saldırganlar, doğrudan cihazın donanımına (USB/Port) fiziksel müdahaleye yönelebilir.
+ Maliyet Tasarrufu: Siber sigorta primlerinde risk azalmasına bağlı indirimler sağlanabilir.	**- Kesinti Riski:** Güvenlik güncellemesi (Patching) sırasında sistemin geçici hizmet dışı kalma ihtimali.

7.2. SMART Hedefler (Çözüm Yol Haritası)

Tespit edilen anomaliyi ortadan kaldırmak için belirlenen aksiyon planı aşağıdaki kriterlere göre oluşturulmuştur:

- S - Specific (Belirli):
  Tüm şarj istasyonları ile sunucu arasındaki haberleşme protokolü, güvensiz ws:// (WebSocket) yapısından, şifreli wss:// (WebSocket Secure) yapısına geçirilecek ve sunucu tarafında "Benzersiz Mesaj ID" (Unique Message ID) kontrolü aktif edilecektir.
- **M - Measurable (Ölçülebilir):**
  - Ağ trafiği analizlerinde (Sniffing testleri) şifrelenmiş paket oranı **%100** seviyesine ulaşmalıdır.
  - Yapılacak sızma testlerinde (Pentest) Replay saldırısı başarı oranı **%0**'a düşürülmelidir.
- A - Achievable (Ulaşılabilir):
  Mevcut şarj istasyonu envanterinin %90'ı OCPP Security Profile 2'yi donanımsal olarak desteklemektedir. Desteklemeyen %10'luk eski cihazlar için harici VPN Gateway donanımları kullanılarak çözüm sağlanacaktır.
- R - Relevant (Amaca Uygun):
  Bu hedef, şirketin "Finansal Kayıpları Önleme" stratejisi ve KVKK (Kişisel Verilerin Korunması Kanunu) uyumluluk süreciyle doğrudan örtüşmektedir.
- T - Time-Bound (Zamanlı):
  Proje takvimi toplam 8 hafta olarak belirlenmiştir:
  - **1-2. Hafta:** Test ortamında WSS ve Sertifika altyapısının kurulumu.
  - **3-4. Hafta:** Pilot bölgedeki 50 istasyonda güncelleme ve canlı testler.
  - **8. Hafta:** Tüm şarj ağının güvenli moda geçişinin tamamlanması ve projenin kapatılması.