# **SWOT ANALİZİ RAPORU**

Konu: Sayaç Değeri (MeterValues) Manipülasyonu ve Hatalı Faturalandırmaya Karşı Savunma Stratejileri

Referans Belge: rapor.md (Sayaç Değerlerinin (MeterValues) Manipülasyonu ve Hatalı Faturalandırma)

Bu analiz, referans belgede tanımlanan "Sayaç Değeri Manipülasyonu" saldırı senaryosuna karşı önerilen savunma ve tespit metodolojilerinin (mTLS, uygulama katmanı imzalama, zaman serisi anomali tespiti vb.) güçlü ve zayıf yönlerini, sektörel fırsatlarını ve bu çözümlere yönelik tehditleri değerlendirmektedir.

## **1. (S) Strengths (Güçlü Yönler)**

*(Önerilen savunma stratejilerinin pozitif içsel özellikleri)*

* Katmanlı Savunma (Defense-in-Depth):  
  Önerilen çözümler tek bir noktaya odaklanmaz. Ağ katmanında (mTLS), uygulama katmanında (Uygulama Katmanı İmzalama) ve sunucu/analiz katmanında (Sunucu Tarafı Anomali Tespiti) koruma sağlayarak katmanlı bir güvenlik mimarisi oluşturur. Bir katman (örn. TLS) aşılsa bile diğer katmanların (örn. imzalama, ML tespiti) saldırıyı yakalama şansı bulunur.
* Proaktif Tespit Yeteneği:  
  Sadece bilinen saldırı imzalarına (imza doğrulaması gibi) güvenmek yerine, Kural T1 (Negatif Tüketim) ve Kural T2 (Şarj Eğrisi Sapması) gibi zaman serisi analizine dayalı makine öğrenimi (ML) yöntemlerinin önerilmesi. Bu, saldırganın daha önce görülmemiş veya "düşük ve yavaş" (low-and-slow) manipülasyon tekniklerini bile proaktif olarak tespit etme potansiyeli sunar.
* Bütünlüğe Odaklanma:  
  Stratejiler (özellikle Uygulama Katmanı İmzalama), saldırının temel hedefi olan "veri bütünlüğünü" (Data Integrity) doğrudan hedefler. Sadece veriyi şifrelemekle kalmayıp, verinin yolda değiştirilmediğini (Tampering) garanti altına almaya çalışır.

## **2. (W) Weaknesses (Zayıf Yönler)**

*(Önerilen savunma stratejilerinin içsel kısıtlamaları veya zorlukları)*

* Yüksek Uygulama ve İşletme Maliyeti:  
  Önerilen mTLS (Karşılıklı TLS) ve Uygulama Katmanı İmzalama çözümleri, güçlü bir Açık Anahtar Altyapısı (PKI) ve sertifika yönetimi süreci gerektirir. Bu sistemlerin kurulumu, bakımı ve milyonlarca cihaza (CP) sertifika dağıtımı operasyonel olarak karmaşık ve maliyetlidir.
* Performans Etkisi (Overhead):  
  Uygulama katmanında (payload) imzalama, her MeterValues mesajı için (potansiyel olarak dakikada bir veya daha sık) kriptografik imzalama (CP tarafında) ve doğrulama (CSMS tarafında) işlemleri gerektirir. Bu durum, özellikle düşük işlem gücüne sahip eski tip şarj cihazları (CP) üzerinde performans sorunlarına yol açabilir.
* ML Modeli Bağımlılığı:  
  Sunucu Tarafı Anomali Tespiti (Kural T1/T2), ML modelinin doğruluğuna kritik düzeyde bağımlıdır. Yetersiz eğitilmiş veya hatalı (false positive) alarm oranı yüksek bir model, operasyonel yüke (gereksiz incelemeler) veya saldırıları kaçırmaya (false negative) neden olabilir.

## **3. (O) Opportunities (Fırsatlar)**

*(Bu savunma stratejilerinin uygulanmasıyla ortaya çıkabilecek dışsal gelişim alanları)*

* Pazar Güveni ve Marka İmajı:  
  Bu kadar güçlü (ve doğrulanabilir) güvenlik önlemlerini uygulayan bir Şarj Noktası Operatörü (CPO), müşterilere ve filo operatörlerine "güvenli ve doğru faturalandırma" garantisi sunarak pazarda rekabet avantajı elde eder ve marka güvenilirliğini artırır.
* Gelişmiş Veri Analitiği için Zemin:  
  Güvenlik amacıyla (Anomali Tespiti) kurulan zaman serisi analiz altyapısı (ML motoru), ileride farklı iş amaçları için de kullanılabilir. Örneğin, şarj istasyonları için kestirimci bakım (predictive maintenance) modelleri veya şebeke için talep tahmini (demand forecasting) gibi katma değerli hizmetler geliştirilebilir.
* Regülasyonlara Öncü Uyum:  
  Gelecekte devletlerin ve düzenleyici kurumların (örn. EPDK) faturalandırma doğruluğu ve siber güvenlik için zorunlu standartlar getirmesi (Avrupa'daki NIS2 direktifi gibi) beklenmektedir. Bu stratejileri şimdiden uygulamak, gelecekteki regülasyonlara kolay uyum sağlar.

## **4. (T) Threats (Tehditler)**

*(Uygulanan savunma stratejilerini etkisiz kılabilecek dışsal riskler)*

* Cihaz Seviyesi Güvenlik Açıkları (Fiziksel Tehditler):  
  Raporda (Madde 4.2 ve 8.4) belirtildiği gibi, ağ (mTLS) ve uygulama (imzalama) ne kadar güvenli olursa olsun, saldırganın şarj cihazına (CP) fiziksel olarak erişmesi veya firmware'ine sızması (örn. Zayıf Cihaz Güvenliği), verinin kaynağından manipüle edilmesine olanak tanır. Bu durumda veri, CSMS'e "geçerli bir imza ile" ve "güvenli bir kanaldan" ama yanlış olarak gönderilir.
* ML Modellerine Yönelik Saldırılar (Adversarial ML):  
  Saldırganlar, ML tabanlı anomali tespit sistemlerinin (Kural T2) çalışma mantığını analiz edebilir. Modeli atlatmak için, tüketim verilerini ani bir düşüşle değil, istatistiksel eşik değerinin hemen altında kalacak şekilde çok yavaş ve uzun bir periyotta (tespit edilemeyecek kadar az) manipüle edebilirler (Adversarial Attack).
* Eski Sistem (Legacy) Entegrasyon Riskleri:  
  Piyasadaki mevcut (legacy) şarj istasyonlarının büyük bir kısmı bu gelişmiş güvenlik protokollerini (mTLS, imzalama) donanımsal veya yazılımsal olarak desteklemeyebilir. Bu durum, operatörleri "ya güvensiz çalışmaya devam etme" ya da "tüm istasyonları yenileme" (yüksek maliyet) ikilemiyle karşı karşıya bırakır.