SWOT Analizi: Elektrikli Araç Şarj İstasyonlarında Güvenlik Zafiyetleri

Kategori	Açıklama
Güçlü Yönler (Strengths)	- OCPP protokolü uluslararası standartlara (OCPP 1.6, ISO 15118) dayandığı için modüler ve yaygın olarak desteklenir. - Cloud–Edge mimarisi sayesinde merkezi kontrol ve yerel işlem gücü dengesi kurulabilir. - NTPsec, SignedMeterValues gibi güvenli zaman ve veri bütünlüğü mekanizmaları kullanılabilir. - Şarj istasyonlarının donanımında fiziksel güvenlik bileşenleri (röle, sayaç, RFID) yer almaktadır.
Zayıf Yönler (Weaknesses)	- Zayıf şifreleme: Bazı sistemlerde TLS veya Mutual TLS doğrulaması etkin değildir. - Yetkisiz erişim: Kimlik doğrulama zafiyetleri nedeniyle yönetim arayüzlerine erişim riski vardır. - Ortadaki Adam (MitM) saldırısı: OCPP trafiği yeterince korunmadığında zaman ve enerji değerleri manipüle edilebilir. - Yazılım açıkları: Güncellenmeyen firmware ve açık kaynak kütüphaneler saldırı yüzeyini artırır. - Zaman farkı veya veri bütünlüğü kontrolünün eksikliği nedeniyle sahte veriler tespit edilemeyebilir.
Fırsatlar (Opportunities)	- Yapay zekâ destekli anomali tespiti ile saldırılar erken aşamada tespit edilebilir. - Güvenli zaman protokolleri (NTPsec, GPS senkronizasyonu) entegre edilerek sektörde fark yaratılabilir. - OCPP ve ISO standartlarına tam uyum, operatörler için güvenlik sertifikasyonu avantajı sağlar. - “Digital Twin” tabanlı simülasyon ortamlarıyla saldırı senaryoları test edilip proaktif savunma stratejileri geliştirilebilir.
Tehditler (Threats)	- Enerji altyapısına yönelik artan siber saldırılar. - Farklı OCPP sürümleri arasındaki güvenlik tutarsızlıkları. - Zaman manipülasyonu gibi gizli saldırıların klasik güvenlik çözümleriyle tespit edilememesi. - Mevzuat eksiklikleri nedeniyle bazı operatörlerin düşük güvenlik standartlarını sürdürmesi.

SMART Hedefler

No	Hedef Başlığı	SMART Tanımı
1.	**Anomali Tespit Modeli Geliştirme**	Şarj istasyonlarından alınan OCPP verilerinde zaman kayması, sahte enerji ölçümü ve veri tekrarları gibi anomalileri en az %95 doğruluk oranı ile tespit edebilen bir yapay zekâ modeli geliştirmek.
2.	**Fiziksel ve Siber Güvenlik Kontrol Listesi Oluşturma**	OCPP 1.6, ISO 15118 ve ISO 27001 standartlarını temel alarak 50 maddelik fiziksel ve siber güvenlik kontrol listesi hazırlamak ve bu listeyi sistemin karar motoruna entegre etmek.
3.	**Enerji Hırsızlığı ve Sahte Veri Enjeksiyonu Algoritması**	Şarj istasyonlarında olağan dışı enerji tüketim desenlerini tespit ederek enerji hırsızlığı ve sahte veri enjeksiyonu vakalarını %90 hassasiyetle belirleyebilen bir analiz algoritması geliştirmek.
4.	**Gerçek Zamanlı Müdahale Modülü Kurulması**	Şüpheli bir aktivite algılandığında sistemin 30 saniye içinde otomatik müdahale (şarj işlemini durdurma veya kullanıcı erişimini sınırlandırma) gerçekleştirmesini sağlayan bir olay yönetim altyapısı kurmak.
5.	**Standartlara Uygunluk ve Uyarlanabilirlik**	Geliştirilen tüm yazılım bileşenlerinin OCPP 1.6, ISO 15118 ve ISO 27001 standartlarıyla %100 uyumlu çalışmasını sağlamak ve güvenli zaman protokollerini (NTPsec, GPS senkronizasyonu) sistemin çekirdek bileşeni haline getirmek.
6.	**Pilot Uygulama ve Test Ortamı Kurulumu**	Geliştirilen güvenlik sistemi ve yapay zekâ modellerini simülasyon veya test istasyonu ortamında çalıştırarak performans, tespit oranı ve yanlış pozitif değerlerini analiz etmek.