SWOT ANALYSİS

Strenghts	Weaknesses	Opportunities	Threats
• Sistematik anomali tespiti (12 farklı senaryo ile kapsamlı analiz) • Veri tabanlı izleme ve log mantığı sayesinde hızlı tanılama • OCPP, NTP, OTA gibi standartlara dayalı yapı — uyumluluk yüksek • Güvenlik tehditlerinin hem donanım hem yazılım boyutunda değerlendirilmesi • "Self-reboot" ve "fail-safe" mekanizmalarıyla dayanıklılık sağlanması	• Sensör, röle ve sayaç gibi donanıma bağımlılık yüksek • OCPP'nin güvenlik katmanı (örneğin TLS konfigürasyonu) hatalara açık • Token yönetimi ve kimlik doğrulama süreçlerinde kullanıcı farkındalığı düşük olabilir • Zaman senkronizasyonu (NTP) ve firmware doğrulaması merkezi sisteme aşırı bağlı • Anomali tespiti gerçek zamanlı çalışmazsa gecikmeli müdahale riski doğar	• Makine öğrenmesi ile anomali tespiti otomatikleştirilebilir. • Blockchain tabanlı işlem kayıtlarıyla güvenlik güçlendirilebilir • Akıllı şehir altyapılarıyla entegrasyon sayesinde veri paylaşımı ve standartlaşma artar • Enerji firmalarıyla iş birliği ile ulusal güvenlik standardı geliştirilebilir • Regülasyonlar ile yatırım fırsatları doğabilir • Mobil uygulamalar ve ödeme sistemleri için Token/Kullanıcı bazlı güvenlik çözümü olarak konumlanma potansiyeli.	• Koordineli yük saldırıları (DDoS benzeri etkiler) enerji altyapısını çökertme riski taşır • Fiziksel sabotaj ve sensör manipülasyonu sonucu veri bütünlüğü kaybı • OTA güncellemelerinde kötü amaçlı firmware enjeksiyonu • Kimlik sahtekarlığı ile kullanıcı zararına işlemler • Zamanla oluşan drift anomalileri fark edilmezse model güvenilirliği azalır • Tarihsel, etiketlenmiş anomali verilerinin yetersizliği nedeniyle AI modelinin başlangıç doğruluğunun düşmesi riski.