SWOT Analizi —

“Evil Twin (Wi-Fi SSID Spoofing) Tabanlı MITM Saldırılarının Dijital Simülasyonla Tespiti ve Yapay Zekâ Destekli Müdahalesi”

Güçlü Yönler (Strengths)

- **Gerçekçi, güvenli simülasyon yaklaşımı:** Fiziksel Wi-Fi kurulumuna ihtiyaç duymadan, izole Docker ortamında MITM davranışlarının kontrollü olarak çoğaltılması güvenlik ve etik açıdan güçlü.
- **Çok katmanlı veri toplama:** Ağ + TLS/DNS + uygulama/telemetri + OCPP (opsiyonel) kombinasyonu daha zengin öznitelik seti sağlar; yanlış pozitifleri düşürme potansiyeli yüksek.
- **Hibrit tespit stratejisi:** Deterministik kurallar + ML (autoencoder, LSTM, Isolation Forest) ensemble ile hem bilineni hem bilinmeyeni yakalama şansı.
- **Açık kaynak teknolojiler kullanımı:** Docker, mitmproxy, OpenSearch, Python ile maliyet düşük, reprodüksiyon ve topluluk desteği kolay.
- **SOC entegrasyonu ve mock-müdahale:** Hem otomatik hem insan destekli süreçleri simüle ederek operasyonel hazırlığı gösterir.

Zayıf Yönler (Weaknesses)

- **Gerçek dünya geçerliliği sınırlılığı:** Simülasyon gerçek AP/firmware/cihaz çeşitliliğinin tüm varyasyonlarını yakalayamayabilir; transferability (modelin gerçek ortama taşınması) riski var.
- **Veri etiketleme ve dengesi:** Anomali/saldırı örneklerinin sınırlı ve sentetik olması model eğitimi ve değerlendirmede yanlılığa yol açabilir.
- **Zaman serisi ve senkronizasyon karmaşıklığı:** Farklı log kaynaklarının zaman damgalarının hizalanması zor olabilir; feature engineering maliyeti artar.
- **False positive maliyeti:** Özellikle otomatik karantina kararları yanlış tetiklenirse operasyonel aksamalara neden olabilir.
- **OCPP ve ödeme iş akışlarına dair sınırlı erişim:** Gerçek OCPP davranışlarını tam taklit etmek zor olabilir; idTag replay kuralları eksik kalabilir.

Fırsatlar (Opportunities)

- **Akademik ve endüstri işbirlikleri:** EV şarj altyapısı operatörleri, OEM’ler ve üniversiteler ile pilot çalışmalar yapılabilir.
- **Modüler ürün/hizmetleşme:** Prototipten SOC entegrasyon eklentileri, eğitim/dokümantasyon paketleri veya test-kiti oluşturularak ticarileşme imkanları.
- **Gelişen regülasyonlar ve siber-fizik güvenlik ihtiyacı:** Kritik altyapı güvenliği farkındalığı arttığı için talep artabilir.
- **Veri zenginleştirme:** Gerçek trafik/telemetri ile (anonimleştirilmiş/pilot) model performansını iyileştirme imkânı.
- **Topluluk katkısı:** Açık kaynak olarak sunulursa güvenlik araştırmacılarından katkı ve test senaryoları gelebilir.

Tehditler (Threats)

- **Etik / hukuki risk algısı:** MITM benzeri tekniklerin simülasyonu yanlış anlaşılırsa hukuki/kurum içi itibar riski oluşabilir. (Proje belgelendirmesi kritik.)
- **Kötüye kullanım endişesi:** Araçlar/kaynak kod saldırganlarca kötüye kullanılmak üzere alınabilir; erişim kontrolü ve lisanslama düşünülmeli.
- **Gerçek dünya saldırı değişkenliği:** Saldırı tekniklerinin evrimi (yeni spoofing/metamask yöntemleri) modelin hızla eskimesine yol açabilir.
- **Operasyonel entegrasyon zorlukları:** Gerçek SOC süreçlerine entegrasyon ve onay alma (OT/ICS ortamlarında) karmaşık olabilir.
- **Regülasyon/standart uyumsuzluğu:** Özellikle ödeme/veri düzenlemeleri ile uyumsuz hareket riskleri (ör. PCI, GDPR benzeri kurallar) var.