PROJE RİSK YÖNETİMİ, STRATEJİLER VE B PLANLARI DÖKÜMANI

Proje Adı: Elektrikli Araç (EV) Şarj İstasyonu Güvenlik ve Anomali Tespit Sistemi
Takım Adı: BSG-1

1. GİRİŞ VE KAPSAM

Bu döküman, **Elektrikli Araç Şarj İstasyonları (EVCS)** için geliştirilen siber güvenlik projesinin 10 haftalık geliştirme sürecindeki riskleri yönetmek amacıyla hazırlanmıştır. Proje iki ana fazdan oluşmaktadır:

1. **Vize (MVP):** Saldırı Simülasyonu (OCPP/CAN üzerinden DoS, Yetkisiz Erişim).
2. **Final:** Savunma ve Anomali Tespiti (Yapay Zeka Destekli IPS ve Dashboard).

Bu plan, simülasyon altyapısı (vcano), veri toplama ve savunma mekanizmalarının geliştirilmesi sırasında oluşabilecek teknik ve zamansal aksaklıklar için **Mühendislik B Planlarını** içerir.

2. RİSK DEĞERLENDİRME MATRİSİ

2.1. Zaman Yönetimi ve Faz Geçiş Riskleri (MVP -> Final)

"Dönüm Noktaları" dosyasındaki sıkışık takvime (Week 6-7 geçişi) yönelik riskler.

Olası Risk Tanımı	Etki (1-5)	Önleme Stratejisi (Proactive)	B Planı (Contingency Plan)
Saldırı Fazına Saplanıp Kalma: Vize haftası (6. Hafta) geldiğinde saldırı scriptlerinin hala stabil çalışmaması ve savunma fazına (7. Hafta) geçilememesi.	5	Saldırı senaryoları sınırlandırıldı. 10 adet yerine **en kritik 2 senaryo** (Örn: Yetkisiz Şarj, DoS) önceliklendirildi.	Savunma sistemi "Otomatik Engelleme (IPS)" yerine **"Pasif İzleme (IDS)"** moduna düşürülecek. Sistem sadece "Uyarı" verecek, engelleme işlemi operatör ekranından manuel yapılacak.

Entegrasyon Gecikmesi: 8. Haftada planlanan "Saldırı" ve "Savunma" modüllerinin birleşirken uyumsuzluk çıkarması.	4	Saldırı ve Savunma ekipleri ortak veri formatı (JSON Log Yapısı) üzerinde en başta anlaştı. Mock (sahte) verilerle testler erken başlatılacak.	Entegrasyon başarısız olursa, sunumda Saldırı ve Savunma modülleri **iki ayrı terminalde** bağımsız çalıştırılacak; birinde saldırı yapılırken diğerinde logların düştüğü manuel gösterilecek.

2.2. Teknik Altyapı ve Simülasyon Riskleri

"Uygulama Senaryosu" ve "Değerlendirme Tasarım" dosyalarındaki teknik detaylara yönelik riskler.

Olası Risk Tanımı	Etki (1-5)	Önleme Stratejisi (Proactive)	B Planı (Contingency Plan)
Sanal Ağ (vcano) Çökmesi: DoS saldırı simülasyonu sırasında sanal CAN veriyolunun veya host makinenin kilitlenmesi.	5	Saldırı scriptlerine "Rate Limiting" (Hız Sınırı) eklendi. Saldırılar izole edilmiş Docker konteynerleri içinde yapılacak.	Canlı DoS demosu iptal edilecek. Bunun yerine saldırının ağ trafiği önceden kaydedilip (PCAP dosyası), sunumda **"Replay" (Tekrar Oynatma)** yöntemiyle sisteme verilecek.
Yapay Zeka Veri Yetersizliği: Anomali tespiti için eğitilecek modelin, sentetik saldırı verilerini "Normal" trafikten ayırt edememesi	4	Saldırı simülasyonları ile kendi veri setimizi üreteceğiz. Ayrıca literatürdeki açık kaynaklı IDS veri setleri (CIC-IDS vb.) ile veri	Yapay zeka modeli başarısız olursa, **Kural Tabanlı (Rule-Based)** algoritmaya geçilecek. (Örn: "Dakikada 100'den fazla istek gelirse

(Overfitting/Underfitting).		zenginleştirme yapılacak.	alarm ver").
Dashboard Veri Gecikmesi: Operatör ekranında (Frontend) saldırı anının saniyeler sonra görünmesi (Latency).	3	WebSocket teknolojisi kullanılarak veri akışı optimize edilecek. Grafik kütüphanesi hafifletilecek.	Canlı grafik çizimi yerine, **"Son Olaylar Listesi"** şeklinde metin tabanlı log akışına dönülecek.

2.3. Kapsam ve Beklenti Riskleri

"Değerlendirme Tasarım" dosyasındaki "Hariç Tutulanlar" bölümüne dayalı riskler.

Olası Risk Tanımı	Etki (1-5)	Önleme Stratejisi (Proactive)	B Planı (Contingency Plan)
Donanım Beklentisi: Jüri veya izleyicilerin fiziksel bir şarj cihazı veya araç görmek istemesi.	3	Proje sunumunun başında "Kapsam: Laboratuvar Simülasyonu" olduğu net bir dille ve görsellerle vurgulanacak.	Fiziksel demo sorulursa, sistemin gerçek dünyadaki karşılığını gösteren **konsept mimari şeması** ve simülasyonun gerçek donanımla nasıl konuşacağını anlatan teknik bir slayt hazırda tutulacak.

3. KRİTİK DÖNÜM NOKTALARI İÇİN B PLANLARI

"Bölüm 7" dosyasındaki kilometre taşlarına özel acil durum planları.

3.1. Dönüm Noktası: MVP - Saldırı Simülasyonu (6. Hafta)

- **Hedef:** DoS ve Yetkisiz Şarj saldırılarını başarıyla çalıştırmak.
- **Risk:** Scriptlerin hedef sistemi (CSMS) etkilememesi.
- **B Planı:** Scriptin çalışmadığı durumda, saldırı etkisini (örneğin şarjın durmasını) manuel

olarak tetikleyen bir "Debug Modu" eklenecek. Jüriye "Saldırı başarılı olduğunda sistem bu tepkiyi verir" mantığı gösterilecek.

3.2. Dönüm Noktası: Final - Otomatik Müdahale / IPS (9. Hafta)

- **Hedef:** Saldırı anında sistemin otomatik bloklama yapması.
- **Risk:** Otomatik müdahalenin yanlışlıkla normal kullanıcıyı bloklaması (False Positive).
- **B Planı:** "Otomatik Bloklama" özelliği varsayılan olarak kapatılacak. Bunun yerine Dashboard üzerine kocaman bir **"SİSTEMİ KİLİTLE"** butonu konularak "İnsan Onaylı Müdahale" mekanizması sunulacak.

4. SONUÇ VE DEĞERLENDİRME

Ekibimiz, bu projenin en büyük zorluğunun **Saldırı Simülasyonundan Savunma Sistemine geçiş (6. ve 7. haftalar)** olduğunun bilincindedir. Bu nedenle, Yapay Zeka modelimiz çalışmasa bile Kural Tabanlı sistemimiz, Otomatik Engelleme çalışmasa bile Manuel Müdahale sistemimiz hazırda bekletilmektedir. Amacımız, her koşulda **çalışan, ölçülebilen ve raporlanabilen** bir mühendislik ürünü ortaya koymaktır.