

Proje Değerlendirme Dökümanı Tasarım

Proje Tanımı

Elektrikli araç şarj istasyonlarında hem fiziksel hem de siber anlamda çeşitli güvenlik tehditleri bulunmaktadır. Bu proje, bu tehditleri tespit etmek, sınıflandırmak, analiz etmek ve yapay zekâ destekli modellerle proaktif olarak önlem alınmasını sağlayan bir güvenlik sistemi geliştirmeyi amaçlamaktadır.

Sistem; şarj istasyonlarından gelen sensör verilerini, ağ kayıtlarını, kamera görüntülerini (opsiyonel) ve sistem loglarını işleyerek güvenlik risklerini algılar, anormal durumları tespit eder ve operatöre anlık uyarılar üretir. Ayrıca, raporlama paneli ile SWOT analizi, risk matrisi ve performans verilerini sunar.

Kapsam

1. Dahil Olanlar

- Elektrikli şarj istasyonlarının güvenlik problemlerinin akademik literatür üzerinden belirlenmesi
- Siber ve fiziksel tehditlerin sınıflandırılması
- Yapay zekâ tabanlı anomali tespit sistemi tasarılanması
- Risk puanı hesaplama algoritması geliştirilmesi
- Yönetim paneli üzerinden olay izleme, raporlama ve uyarılar
- Makale tarama (Connected Papers, ResearchRabbit) + her grup üyesi tarafından makale incelemesi
- SMART hedefler, SWOT analizi ve risk analiz dokümanlarının oluşturulması

2. Hariç Tutulanlar

- Gerçek fiziksel istasyon kurulumu
- Ticari bir ürün geliştirme
- Tam anlamıyla gerçek zamanlı ulusal altyapı entegrasyonu

Sistem Mimarisi

1. Veri Toplama Katmanı

- Şarj istasyonundan gelen sensör verileri
- Ağ trafiği logları
- Operasyonel kayıtlar
- (İsteğe bağlı) Kamera veya IoT cihaz verileri

2. Yapay Zekâ Analiz Katmanı

- Makine öğrenimi tabanlı anomali tespit modeli
- Tehdit sınıflandırma modülü
- Risk puanı hesaplama algoritması
- Veri ön işleme + model güncellemeleri

3. Uyarı ve Olay Yönetimi Katmanı

- Kritik seviyede tehdit algılandığında otomatik bildirim
- Operatör için uyarı ekranı
- Olay geçmişi ve loglama

4. Raporlama ve Dashboard Arayüzü

- Güncel istasyon durumu
- Günlük/haftalık risk raporları
- SWOT, SMART, risk matrisi gibi proje raporlamaları
- Grafiksel veri görselleştirme

4. Kullanıcı Profilleri

4.1. Sistem Yöneticisi

- Yapay zekâ modelini yönetir
- Logları ve raporları inceler
- Sistem ayarlarını düzenler
- Güvenlik olaylarını analiz eder

4.2. Operatör / Gözlemci

- Dashboard üzerinden canlı veriyi takip eder
- Uyarıları alır ve olaya müdahale eder
- Şarj istasyonunun günlük risk durumunu izler

4.3. Araştırmacı / Akademik Kullanıcı

- Makale sonuçlarını sisteme ekler
- Güvenlik açıkları listesini günceller
- Analiz raporlarını üretir

4.4. Son Kullanıcı (EV Driver – opsiyonel)

(Güvenlik öncelikli proje olduğu için kullanıcı etkileşimi yoktur; sadece bilgi amaçlı eklenmiştir.)

- İstasyonda olası güvenlik durumları hakkında bilgilendirilebilir

5. Süreç Akışı

5.1. Temel İş Akış Adımları

1. Veri Toplama

Şarj istasyonundan sürekli olarak sensör verileri, loglar ve ağ trafiği toplanır.

2. Veri İşleme ve Analiz

Veri makine öğrenimi modellerine iletilir; normal ve anormal davranışlar karşılaştırılır.

3. Anomali / Tehdit Tespiti

Yapay zekâ modeli risk seviyesini hesaplar:

- Düşük Risk
- Orta Risk
- Yüksek Risk (Alarm oluşturulur)

4. Uyarı ve Bildirim

Sistem yönetici ve operatör dashboard üzerinden bilgilendirilir.

5. Olay Yönetimi

Operatör olayı değerlendirir, not ekler, çözüm adımlarını işaretler.

6. Raporlama

Sistem tarafından otomatik raporlar:

- Günlük risk raporu
- Haftalık analiz
- Aylık istasyon performansı

7. Akademik Destek ve Genişletme

Her ekip üyesinin incelediği makaleler sisteme entegre edilerek yeni riskler eklenir.

Bölüm 7: Dönüm Noktaları ve Kilometre Taşları

7.1. MVP (Minimum Uygulanabilir Ürün) Tanımı

Projemizin MVP'si (Vize Dönemi Sürümü), Elektrikli Araç Şarj İstasyonlarına (EVCS) yönelik siber saldırıların laboratuvar ortamında başarıyla simüle edildiği **"Siber Anomali Test Altyapısı"**dir.

MVP sürümü (v1.0) şunları kapsar:

- Simülasyon Ortamı:** Şarj istasyonu ve yönetim sistemi arasındaki haberleşmenin sanal ortamda taklit edilmesi.
- Saldırı Senaryoları:** Belirlenen öncelikli anomalilerin (Örn: DoS, Yetkisiz Şarj Başlatma) sistem üzerinde çalıştırılması.
- Zafiyet Kanıtı:** Yapılan saldırıların sistemde oluşturduğu etkinin (hizmet kesintisi vb.) doğrulanması.

7.2. Zorlayıcı Hedefler (Stretch Goals)

Vize dönemi sonrası (Final Sürümü için) asıl hedefimiz, bu saldırıları engelleyen çözümü geliştirmektir:

- Savunma Uygulaması:** Simüle edilen saldırıları gerçek zamanlı tespit edip engelleyen güvenlik yazılımının geliştirilmesi.
- Otomatik Müdahale (IPS):** Saldırı anında sistemin otomatik olarak güvenli moda geçmesi ve saldırıcı bloklaması.
- Yönetici Paneli (Dashboard):** Saldırı ve savunma durumlarını gösteren görsel arayüz tasarımı.
- Tam Entegrasyon:** Projedeki tüm anomali senaryolarının (10 adet) tek bir sistemde hem saldırı hem savunma yönüyle çalışır hale gelmesi.

7.3. Kilometre Taşları ve Proje Programı (Timeline)

Bu çizelge, 6. haftaya kadar **saldırı simülasyonlarının (MVP)** tamamlanmasını, ardından final dönemine kadar bu saldırılara karşı **savunma uygulamasının** geliştirilmesini içerir.

Hafta	Odak Noktası	Tamamlanan Kilometre Taşı (Somut Çıktı)
1. Hafta	Literatür ve Kapsam	Elektrikli araç şarj istasyonları (CSMS, OCPP) güvenlik açıkları literatür taraması tamamlandı. Proje kapsamı netleştirildi.
2. Hafta	Senaryo Belirleme	Simüle edilecek anomali senaryoları (Örn: DDoS, Enerji Kesme) belirlendi. Ekip görev dağılımı yapıldı.
3. Hafta	Analiz (SWOT/SMART)	Seçilen anomaliler için SWOT Analizleri ve bunlara karşı hedeflenen çözüm stratejileri (SMART Hedefler) dokümantة edilip Github'a yüklandı.
4. Hafta	Altyapı Kurulumu	Saldırıların gerçekleştirileceği sanal laboratuvar ortamı (Ubuntu/Server vb.) kuruldu ve ağ yapılandırması tamamlandı.
5. Hafta	Saldırı Scriptleri	Belirlenen öncelikli anomalilerin (İlk grup saldırılar) kodları/scriptleri yazıldı ve bireysel testleri yapıldı.
6. Hafta	Vize Sürümü (MVP)	MVP (Saldırı Fazı) Tamamlandı. Şarj istasyonuna yönelik belirlenen saldırı senaryoları simülasyon ortamında başarıyla çalıştırıldı ve sonuçları doğrulandı.
7. Hafta	Savunma Geliştirme	Vize sonrası, saldırıları tespit edecek "Güvenlik Uygulaması"nın mimarisi tasarlandı ve temel kodlamasına başlandı.
8. Hafta	Entegrasyon	Geliştirilen savunma modülü (Beta) sisteme eklendi. Saldırı yapıldığında uygulamanın tespit/loglama yaptığı görüldü.
9. Hafta	Otomasyon ve Arayüz	Uygulamaya otomatik engelleme (Bloklama) özelliği ve görsel panel (Dashboard) eklendi. Stres testleri yapıldı.
10. Hafta	Final Teslimi	Tüm sistemi (Saldırı + Savunma) kapsayan Demo Videosu, Kullanım Kılavuzu ve Proje Sonuç Raporu tamamlanarak teslim edildi.

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:

- Vize (MVP):** Saldırı Simülasyonu (OCPP/CAN üzerinden DoS, Yetkisiz Erişim).
- 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 aksaklılıklar 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 geçiş) 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 Engellemeye (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 yapılmırken 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 saldırısı 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 çalışırmak.
- Risk:** Scriptlerin hedef sistemi (CSMS) etkilememesi.
- B Planı:** Scriptin çalışmadığı durumda, saldırı etkisini (örneğin şarjin 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

Ekipimiz, bu projenin en büyük zorluğunu **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.