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"**dır.

MVP sürümü (v1.0) şunları kapsar:

1. **Simülasyon Ortamı:** Şarj istasyonu ve yönetim sistemi arasındaki haberleşmenin sanal ortamda taklit edilmesi.
2. **Saldırı Senaryoları:** Belirlenen öncelikli anomalilerin (Örn: DoS, Yetkisiz Şarj Başlatma) sistem üzerinde çalıştırılması.
3. **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:

1. **Savunma Uygulaması:** Simüle edilen saldırıları gerçek zamanlı tespit edip engelleyen güvenlik yazılımının geliştirilmesi.
2. **Otomatik Müdahale (IPS):** Saldırı anında sistemin otomatik olarak güvenli moda geçmesi ve saldırganı bloklaması.
3. **Yönetici Paneli (Dashboard):** Saldırı ve savunma durumlarını gösteren görsel arayüz tasarımı.
4. **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**) dokümante edilip Github'a yüklendi.
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.