PROJEYE GENEL BAKIŞ DÖKÜMANI

Tanımlama

- Proje Adı: CHARGE-SHIELD AI
- Proje liderinin adı ve e-posta adresi: Salih Emin Töre / 235541022@firat.edu.tr
- Ekip üyesi isimleri ve e-posta adresleri:

Ad Soyad	E-posta
Semih Gümüş	215541020@firat.edu.tr
Melik Fırat Çenber	225541026@firat.edu.tr
Hasan Sido	225541601@firat.edu.tr
Berat Erol	235541010@firat.edu.tr
Emin Töre	235541022@firat.edu.tr
Kadir Başer	235541036@firat.edu.tr
Ahmet Turan Doğan	235541053@firat.edu.tr
Merve Özberk	235541072@firat.edu.tr
Berçem Biçer	235541094@firat.edu.tr
Mahmut Dağaşan	235541126@firat.edu.tr
Ömer Gülnaroğlu	235542011@firat.edu.tr
İbrahim Halil Yılmaz	245541022@firat.edu.tr

- GitHub Linkimiz: https://github.com/salihtore/EVSE-Security-Lab

Asansör Konuşması

Elektrikli araç şarj istasyonları hızla yayılırken, kullanıcılar **oturum çalma** ve **yetkisiz erişim** gibi kritik siber güvenlik riskleriyle karşı karşıya kalıyor. Projemiz olan **Elektrikli Şarj İstasyonlarının güveliği**, elektrikli araç kullanıcılarının şarj işlemlerini **tamamen güvenli** bir şekilde tamamlamasını garanti eden akıllı bir güvenlik platformudur. Sunduğumuz önlemler, yetkisiz erişimleri ve dolandırıcılığı anında engelleyerek, hem kullanıcının finansal ve kişisel haklarını koruyor hem de şarj istasyonu işletmecilerinin kesintisiz ve **verimli bir altyapı yönetimi** yapmasını sağlıyor.

PROJE GENEL BAKIŞ VE YÖNETİM DOSYASI

1. PROJE KÜNYESİ (TEAM CHARTER)

Proje Adı: CHARGE-SHIELD AI **Vizyon :** Elektrikli araç şarj ekosistemini siber tehditlere karşı koruyan, yapay zeka destekli proaktif bir güvenlik kalkanı olmak.

Proje Lideri: Emin Töre (235541022@firat.edu.tr)

Proje Ekibi: Bu proje, uzmanlık alanlarına göre aşağıdaki gibi iş paketlerine (İP) ayrılarak yürütülmektedir:

Ad Soyad	Görev / Uzmanlık Alanı
Semih Gümüş	**Backend & AI Model Entegrasyonu**
Melik Fırat Çenber	**Anomali Senaryoları & Test**
Hasan Sido	**Risk Analizi & Dokümantasyon**
Berat Erol	**Veri Toplama & Dataset Hazırlığı**
Emin Töre	**OCPP Protokol Güvenliği** (Auth Bypass)
Kadir Başer	**Simülasyon Ortamı** (Network)
Ahmet Turan Doğan	**Sensör Verisi Anomalileri**
Merve Özberk	**Literatür Taraması & Raporlama**
Berçem Biçer	**Frontend & Dashboard Tasarımı**
Mahmut Dağasan	**Saldırı Script'leri** (Red Team)

Ömer Gülnaroğlu	**Sistem Mimarisi & Entegrasyon**
İbrahim Halil Yılmaz	**Test & Kalite Güvence** (QA)

2. YÖNETİCİ ÖZETİ (EXECUTIVE SUMMARY)

Elektrikli araç şarj istasyonları (EVSE) hızla yayılırken, kullanıcılar **"oturum çalma"**, **"yetkisiz erişim"** ve **"enerji hırsızlığı"** gibi kritik siber güvenlik riskleriyle karşı karşıya kalmaktadır. Mevcut güvenlik çözümleri genellikle reaktif (olay sonrası) çalışmaktadır.

CHARGE-SHIELD AI, elektrikli araç kullanıcılarının şarj işlemlerini güvenli tamamlamasını garanti eden akıllı bir güvenlik platformudur. Proje, **Yapay Zeka** ve **Durum Bazlı Analiz** yöntemlerini kullanarak saldırıları milisaniyeler içinde tespit eder ve **otomatik müdahale (IPS)** yeteneği ile işlemi durdurarak finansal kaybı önler.

3. TEKNİK MİMARİ VE KAPSAM

3.1. Sistem İşleyişi (Data Flow)

1. **Veri Toplama:** Şarj istasyonundan gelen sensör verileri, ağ logları ve OCPP mesajları toplanır.
2. **Analiz (AI Core):** Veriler Python tabanlı Anomali Tespit Motoruna iletilir.
3. **Karar:** Normal ve Anormal davranışlar karşılaştırılır. Risk Puanı hesaplanır.
4. **Müdahale:** Risk yüksekse, sistem otomatik olarak RemoteStopTransaction komutu gönderir.

3.2. Kapsam Dışı (Out of Scope)

- Gerçek, fiziksel bir 22kW AC şarj istasyonu üretimi/kurulumu.
- Ticari bir ödeme sistemi entegrasyonu.
- Ulusal elektrik şebekesine (Grid) tam entegrasyon.

GEREKSİNİM ANALİZİ

Bölüm 1: İşlevsel Gereksinimler (Sistemin Ne Yaptığı)

1.1. Siber Anomali Test Altyapısı (MVP - Saldırı Fazı)

ID	Gereksinim	Açıklama
FR-S.1	Simülasyon Ortamı Kurulumu	Sistem, bir şarj istasyonu (Charge Point) ve bir merkezi yönetim sistemi (CSMS) arasındaki **OCPP iletişimini** sanal ortamda taklit etmelidir.
FR-S.2	Saldırı Script'i Çalıştırma	Sistem, belirlenen anomalilere (Örn: **Denial of Service - DoS, Yetkisiz Şarj Başlatma**) yönelik özelleştirilmiş saldırı script'lerini çalıştırabilmelidir.
FR-S.3	Zarifet Doğrulama	Saldırı sonrası, sistem simülasyon ortamındaki şarj/hizmet kesintisi, enerji tüketimi anomalisi gibi **somut etkileri** loglayarak kanıtlamalıdır.

1.2. Savunma ve Engelleme Uygulaması (Final - Savunma Fazı)

ID	Gereksinim	Açıklama
FR-D.1	Gerçek Zamanlı Tespit	Savunma uygulaması, şarj istasyonu ile CSMS arasındaki tüm **OCPP trafiğini** gerçek zamanlı olarak izlemeli ve anomali tespiti yapmalıdır.
FR-D.2	Otomatik Engelleme (IPS)	Tespit edilen saldırı anında, sistem protokol bazında (IP/Port yerine anormal paketi) engellemeli ve saldırganın sisteme erişimini **otomatik olarak bloklamalıdır**.
FR-D.3	Güvenli Moda Geçiş	Kritik bir **DoS saldırısı** tespit edildiğinde, sistem şarj istasyonunu otomatik olarak **"Güvenli Moda"** (bekleme/hizmet dışı) geçirebilmelidir.

FR-D.4	Durum Raporlama ve Loglama	Tüm saldırı olayları, engelleme eylemleri ve sistem durumu, daha sonra analiz edilmek üzere detaylı olarak **zaman damgasıyla** loglanmalıdır.

Bölüm 2: İşlevsel Olmayan Gereksinimler (Sistemin Nasıl Çalıştığı)

Madde	Kategori	Gereksinim Detayı
NFR-1	**Performans**	Savunma modülünün, OCPP trafiği izleme ve engelleme sırasında şarj işleminin normal gecikmesinin (**latency**) **50 ms'nin altında** tutması gerekir.
NFR-2	**Güvenilirlik**	Savunma uygulaması, sürekli olarak (24/7) çalışabilmeli ve bir saldırı anında **%99.9** oranında doğru tespit ve engelleme sağlamalıdır.
NFR-3	**Güvenlik (Kendi Güvenliği)**	Savunma modülünün kendisi, devre dışı bırakma veya manipülasyon amaçlı saldırılara karşı korunmuş olmalıdır.
NFR-4	**Kullanılabilirlik**	**Yönetici Paneli (Dashboard)**, güncel saldırı/savunma durumunu tek bir ekranda, kolay anlaşılır grafiklerle göstermelidir.
NFR-5	**Sürdürülebilirlik**	Geliştirilen tüm kodlar, kolayca güncellenebilir ve genişletilebilir yapıda olmalıdır (Örn: Yeni anomali senaryoları eklemek için).

Bölüm 3: Arayüz Gereksinimleri

3.1. Yönetici Paneli Arayüzü (Dashboard)

1. Görselleştirme: Toplam saldırı sayısı, engellenen saldırı türleri, anlık trafik durumu ve şarj istasyonu sağlık durumu gösterilmelidir.
2. Bildirimler: Kritik bir saldırı tespit edildiğinde anlık görsel ve sesli uyarılar sağlanmalıdır.
3. Raporlama: Belirli bir zaman dilimine ait (günlük/haftalık/aylık) saldırı ve engelleme raporları PDF veya CSV formatında dışa aktarılabilmelidir.

İşlevsellik
Elektrikli Şarj İstasyonu Güvenlik Platformu

1. Temel Güvenli Şarj İşlemi

Bu senaryo, kullanıcıların oturum çalma ve yetkisiz erişim gibi kritik siber güvenlik riskleri olmadan şarj işlemlerini tamamlamasını garanti eden ana işlevi kapsar.

Adım	Aktör	Eylem	Sistemin Yanıtı
1	EA Kullanıcısı	Şarj istasyonuna ulaşır ve EA'yı bağlar.	-
2	EA Kullanıcısı	Platform üzerinden kimlik doğrulama başlatır (örn. uygulama, RFID, QR kod).	Sistem, kullanıcı kimliğini ve yetkilendirmeyi doğrular.
3	Güvenlik Platformu	Şarj oturumunu başlatmadan önce, istasyon ve kullanıcı arasındaki iletişimi güvence altına alır.	İletişim tüneli oluşturulur ve şarj oturumu başlatılır.
4	EA Kullanıcısı	Şarj işlemi başlar.	Platform, şarj oturumu boyunca yetkisiz erişim ve oturum çalma girişimlerini **anında engeller**[22].
5	EA Kullanıcısı	Şarjı sonlandırır.	Şarj verileri ve işlem bilgileri güvenli bir şekilde işlenir ve kullanıcıya iletilir.

2. Yetkisiz Erişim ve Dolandırıcılığı Engelleme

Bu senaryo, platformun kullanıcının finansal ve kişisel haklarını korumak ve şarj istasyonu işletmecilerinin verimli altyapı yönetimini sağlamak için sunduğu temel önlemleri detaylandırır.

Adım	Aktör	Eylem	Sistemin Yanıtı
1	Güvenlik Platformu	Sürekli İzleme ve Analiz yapar.	Tüm şarj istasyonlarından ve oturumlarından gelen veri akışını sürekli olarak izler.
2	Potansiyel Saldırgan	Oturum çalma veya yetkisiz bir erişim girişimi yapar.	Platform, anormallikleri (IP adresi değişikliği, beklenmedik veri paketleri vb.) anında tespit eder[4].
3	Güvenlik Platformu	Saldırıyı Engeller.	Tespit edilen yetkisiz erişim veya dolandırıcılık girişimini **anında bloke eder** ve şarj işlemini durdurur[5].
4	Güvenlik Platformu	Uyarı ve Raporlama.	İstasyon işletmecisine ve/veya ilgili kullanıcıya güvenlik ihlali girişimi hakkında anlık bildirim gönderir.

3. İşletmeci İçin Kesintisiz ve Verimli Altyapı Yönetimi

Bu senaryo, güvenlik platformunun şarj istasyonu işletmecilerine sunduğu kesintisiz ve **verimli bir altyapı yönetimi** imkanını gösterir.

Adım	Aktör	Eylem	Sistemin Yanıtı
1	İstasyon İşletmecisi	Güvenlik Paneline Erişir.	Platforma özgü güvenli bir yönetim arayüzü (web/mobil) üzerinden oturum açar.
2	İstasyon İşletmecisi	Altyapı Durumunu Görüntüler.	Tüm şarj istasyonlarının mevcut güvenlik durumunu, aktif oturumları ve geçmiş ihlal kayıtlarını tek bir yerden izler.
3	Güvenlik Platformu	Güvenlik Yamalarını	Şarj istasyonu yazılımlarındaki güvenlik açıklarını otomatik olarak tespit eder ve

		Otomatik Uygular.	gerekli güncellemeleri, istasyonun çalışmasını aksatmayacak şekilde yükler.
4	İstasyon İşletmecisi	Rapor Oluşturur.	Güvenlik olayları, engellenen dolandırıcılık girişimleri ve sistem performansı hakkında periyodik veya talep üzerine raporlar oluşturur.

Bu kullanım durumları, projenin kritik siber güvenlik risklerini ele alan ve **tamamen güvenli** bir şarj deneyimi sağlayan temel işlevlerine odaklanmaktadır.