

⚡ Elektrikli Araç Şarj İstasyonlarında (CSMS) Anomali Tespiti Başarısı

Metin: Ekip olarak geliştirdiğimiz projede kritik bir aşamayı daha tamamladık: OCPP Schema Drift ve Flood Saldırı Senaryoları.

Bir şarj istasyonuna, standartlara uymayan veri tipleri (örneğin sayı yerine metin) gönderildiğinde veya sistem yoğun veri trafiğine maruz bırakıldığında ne olur? Biz bu sorunun cevabını güvenli bir ortamda simüle ettik.

Yaptığımız testlerde:

1. Hatalı Veri Enjeksiyonu: Sistemin veri doğrulama mekanizmasını zorladık.
2. Yüksek Frekanslı Trafik: Sistemin dayanıklılığını test ettim.

Geliştirdiğimiz güvenlik algoritmaları, bu anomalileri milisaniyeler içinde yakalayarak operatör panelinde gerekli uyarıları (Alert) oluşturdu. Bu simülasyon, gerçek dünyadaki siber tehditlere karşı sistemimizin ne kadar hazırlıklı olduğunu kanıtlıyor.

Emeği geçen tüm ekip arkadaşımıza teşekkürler! 🙌







SENARYO AÇIKLAMASI

Bu senaryoda, Elektrikli Araç Şarj İstasyonu (EVSE) ile Merkezi Yönetim Sistemi (CSMS) arasındaki haberleşme güvenliğini test etmek amacıyla '**OCPP Schema Drift**' saldırısı simüle edilmiştir.

Saldırı kapsamında, sisteme standartlara uygun olmayan veri tipleri (örneğin; tam sayı olması gereken connectorId alanına 'string' veri girilmesi) enjekte edilmiştir. Ayrıca, bu hatalı paketlerin sistem tarafından gözden kaçırılmaması ve IDS'in (Saldırı Tespit Sistemi) tepki süresini ölçmek adına, paketler yüksek frekansta gönderilerek sistemin anomali yakalama kabiliyeti doğrulanmıştır.