

⚡ 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.

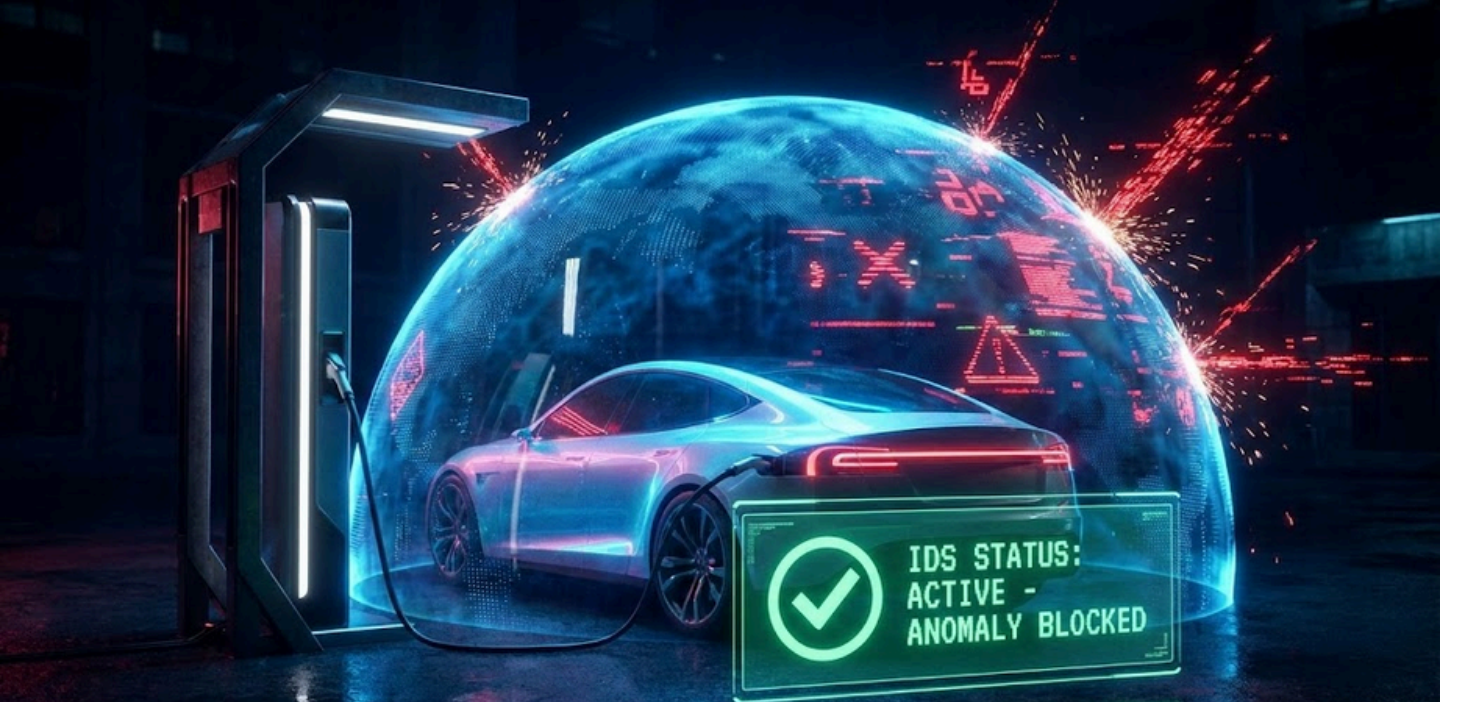
Bir şarj istasyonuna, standartlara uymayan veri tipleri (örneğin sayı yerine metin) gönderildiğinde veya sistem yoğun veri trafiğine maruz bırakıldığında ne olur? Biz bu sorunun cevabını güvenli bir ortamda simüle ettik.

Yaptığımız testlerde:

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

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 arkadaşlarıma teşekkürler! 🌟

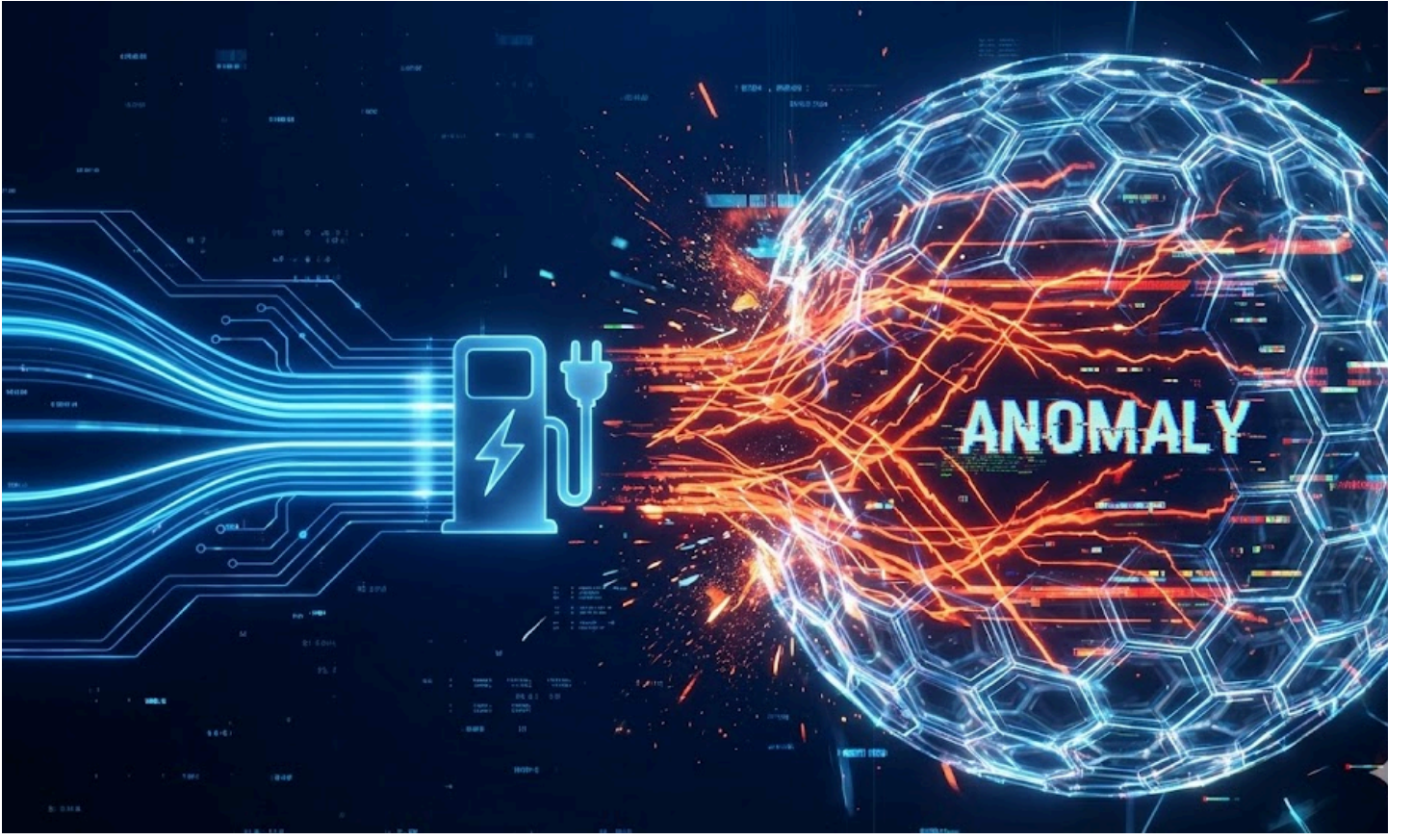




ALERT: OCPP ANOMALY DETECTED

TYPE: Schema Mismatch / High Frequency

ID	Protocol	Device/Location	Health/Status	Priority	Size	Timestamp	Owner
1001001-16-01-001	OCPP	Station 1	OK	3	1024	2023-10-26 10:00:00	Admin
1001001-16-01-002	OCPP	Station 2	Warning	4	2048	2023-10-26 10:05:00	Admin
1001001-16-01-003	OCPP	Station 3	Warning	4	1024	2023-10-26 10:10:00	Admin
1001001-16-01-004	OCPP	Station 4	OK	3	1024	2023-10-26 10:15:00	Admin
1001001-16-01-005	OCPP	Station 5	Warning	4	2048	2023-10-26 10:20:00	Admin
1001001-16-01-006	OCPP	Station 6	Warning	4	1024	2023-10-26 10:25:00	Admin
1001001-16-01-007	OCPP	Station 7	Warning	4	1024	2023-10-26 10:30:00	Admin
1001001-16-01-008	OCPP	Station 8	Warning	4	1024	2023-10-26 10:35:00	Admin
1001001-16-01-009	OCPP	Station 9	Warning	4	1024	2023-10-26 10:40:00	Admin
1001001-16-01-010	OCPP	Station 10	Warning	4	1024	2023-10-26 10:45:00	Admin



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.