📝 LinkedIn Post Taslağı

Başlık: Şarj İstasyonlarında Siber Güvenlik: OCPP Mesaj Yoğunluğu Saldırılarına Karşı Hazır mıyız? ⚡🔐

Elektrikli araç (EV) ekosistemi büyürken, şarj altyapılarının siber dayanıklılığı her zamankinden daha kritik hale geliyor. Bugün, ekibimizle birlikte en yaygın tehditlerden biri olan **OCPP Mesaj Yoğunluğu (DoS Hazırlığı)** saldırısını simüle ettik! 🚀

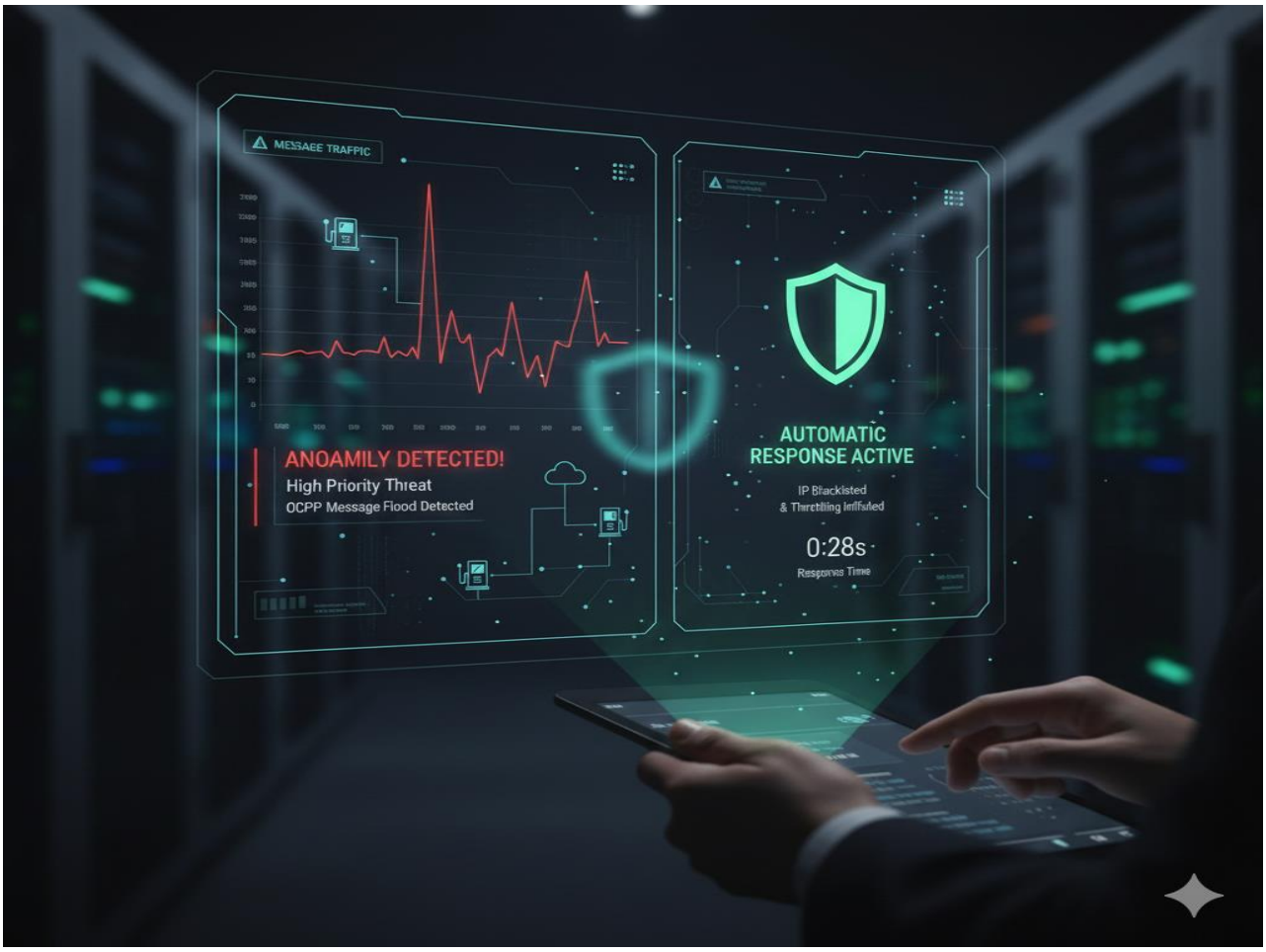
Peki, nedir bu senaryo? Bir saldırganın, ele geçirilmiş bir şarj istasyonu üzerinden Merkezi Yönetim Sistemine (CSMS) saniyeler içinde yüzlerce anlamsız Heartbeat.req veya StatusNotification.req mesajı pompaladığını hayal edin. Amaç; sistemi kilitlemek, diğer istasyonların iletişimini kesmek ve hizmeti durdurmaktır.

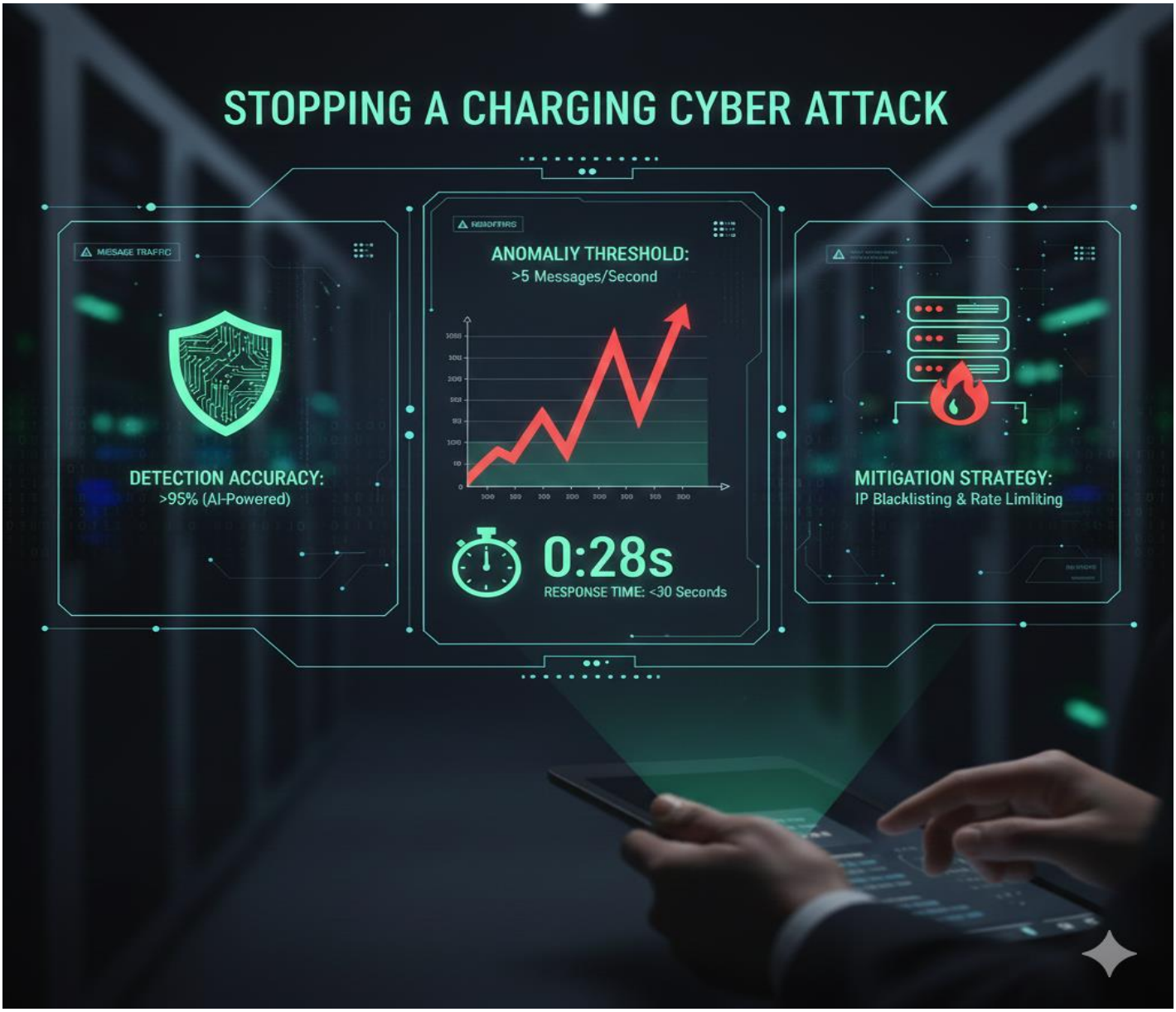
Simülasyonda Neleri Test Ettik?

- **Yapay Zeka Destekli Tespit:** Sistemimiz, mesaj hacmindeki ani sapmaları (spike) **≥%95 doğrulukla** anında yakalayabiliyor mu?
- **Hızlı Müdahale:** Anomali tespit edildikten sonra **30 saniye içinde** otomatik engelleme (throttling/karaliste) aksiyonu devreye giriyor mu?

Sonuç: Geliştirdiğimiz anomali tespit algoritmaları ve Rate Limiting stratejileri sayesinde, siber saldırıları daha operasyona zarar vermeden durdurmayı hedefliyoruz. Dijitalleşen enerji dünyasında güvenliği bir adım önde tutmaya devam ediyoruz!

#EVCharging #CyberSecurity #OCPP #SmartGrid #IoT #SiberGüvenlik #AnomaliTespiti #CSMS




STOPPING A CHARGING CYBER ATTACK
DETECTION ACCURACY:
>95% (AI-Powered)
ANOMALIY THRESHOLD:
>5 Messages/Second
0:28s
RESPONSE TIME: <30 Seconds
MITIGATION STRATEGY:
IP Blacklisting & Rate Limiting