SWOT Analizi – AD-GS ile Tespit Edilen DDoS Tabanlı Anomali Senaryosu

Bu SWOT analizi, Grid Sentinel (AD-GS) çerçevesi kullanılarak tespit edilen, EV şarj yönetim sistemine yönelik DDoS saldırısı senaryosunu esas alır. Analiz; akıllı şebeke altyapısında, sahte ve yoğun şarj talepleriyle iletişim kanallarının ve işlem kaynaklarının aşırı yüklenmesi sonucu ortaya çıkan anomalinin, teknik, operasyonel ve güvenlik boyutlarını akademik bir çerçevede değerlendirmektedir. Temel bulgular, Kesavan vd. (2025) çalışmasındaki simülasyon sonuçlarına dayanmaktadır. Nature+1

Güçlü Yönler (Strengths)

- **Yüksek Hassasiyetli Anomali Tespiti:**
  AD-GS, normal trafik modeli ile anormal (sahte ve yüksek yoğunluklu) talepler arasındaki sapmaları zaman serisi ve davranışsal özellikler üzerinden analiz ederek yüksek doğruluk oranlarıyla (≈%96.8) DDoS aktivitesini tespit edebilmektedir. Nature
- **Gerçek Zamanlı İzleme ve Düşük Gecikme:**
  Çerçeve, iletişim ve istek yoğunluğundaki olağandışı artışları milisaniye mertebesinde işleyerek (<15 ms seviyesinde raporlanan tepki süreleriyle) hizmet kesintisi yaşanmadan önce operatöre uyarı üretme potansiyeline sahiptir; bu da DDoS kaynaklı kesinti süresini ve etki alanını azaltır. Nature+1
- **Yük Eşiği ve Kapasite Farkındalığı:**
  Normal yük profillerine dayalı referans eşikleri sayesinde, sistem; saldırı kaynaklı yapay yüklenme ile gerçek talep artışını ayırt edebilen, bağlama duyarlı bir karar mekanizması geliştirme imkânı sunar.
- **Merkezi Yönetim ile Entegrasyon:**
  AD-GS, merkezi şarj yönetim sistemi ve akıllı şebeke denetim katmanına entegre edilerek; saldırı tespiti sonrası otomatik trafik sınırlama, isteği düşürme, yeniden yönlendirme veya belirli istasyonları izole etme gibi tepki politikalarının orkestrasyonunu destekler.

Zayıf Yönler (Weaknesses)

- **Normal Trafiğin Doğru Modellenmesine Bağımlılık:**
  DDoS tespit performansı, "normal" şarj talebi desenlerinin doğru ve güncel modellenmesine kritik derecede bağlıdır. Yoğun saatler, kampanyalar veya bölgesel talep patlamaları, model güncellenmezse yanlış pozitiflere yol açabilir.
- **Dağıtık ve Yavaş-Oranlı Saldırılara Karşı Sınırlılıklar:**
  Birçok istasyona yayılmış, düşük oranlı ancak koordineli saldırılar (low-rate veya stealthy DDoS) normal desene yakın görünebilir; yalnızca hacim temelli eşiklere dayanan modeller bu saldırıları kaçırabilir veya geç tespit edebilir.
- **Veri ve Altyapı Bağımlılığı:**
  Hızlı ve güvenilir tespit için kapsamlı loglama, zaman senkronizasyonu, yeterli işlem gücü ve güvenli iletişim altyapısı gereklidir. Zayıf donanım, eksik izleme veya hatalı konfigürasyon, AD-GS'in etkinliğini düşürebilir.

- **Yanlış Pozitiflerin Operasyonel Yükü:**
  Normal talep dalgalanmalarının saldırı olarak işaretlenmesi; gereksiz kısıtlamalar, meşru kullanıcıların engellenmesi ve operasyon ekiplerinde "alarm yorgunluğu" oluşturarak sistemin güvenilir algısını zedeleyebilir.

Fırsatlar (Opportunities)

- **Mikro Hizmet Kesintilerini Azaltan Proaktif Savunma:**
  DDoS anomalilerinin erken tespiti, hizmet sağlayıcıların SLA'leri korumasına, istasyon kullanılabilirliğini artırmasına ve kullanıcı memnuniyetini güçlendirmesine imkân tanır; bu da rekabetçi avantaj sağlar.
- **Politika Tabanlı Otomatik Müdahale Mekanizmaları:**
  AD-GS çıktıları; SDN tabanlı trafik yönetimi, oran sınırlama, IP/istasyon kara listeleme, yük dengeleme ve talep şekillendirme stratejileriyle entegre edilerek otonom savunma katmanları geliştirmek için kullanılabilir.
- **Standardizasyon ve Regülasyonla Uyumlu Güvenlik Çerçeveleri:**
  DDoS tespitine yönelik ölçülebilir performans göstergeleri (doğruluk, gecikme, veri bütünlüğü) sunan bir framework, gelecekteki akıllı şebeke güvenlik standartları ve sertifikasyon süreçlerine referans model olarak entegre edilebilir.
- **Diğer Saldırı Tiplerine Genellenebilirlik:**
  DDoS senaryosu için eğitilen ve doğrulanan anomali tespit mimarisi; uygun özellik mühendisliği ile yanlış veri enjeksiyonu, yetkisiz erişim veya protokol suistimali gibi diğer saldırı sınıflarına genişletilerek bütüncül bir savunma platformuna dönüştürülebilir. ResearchGate

Tehditler (Threats)

- **Uyarlanabilir ve Adversarial Saldırı Teknikleri:**
  Saldırganlar, AD-GS'in karar sınırlarını öğrenerek trafik desenlerini buna göre uyarlayabilir, adversarial örnekler üretebilir veya veri zehirleme yoluyla modelin karar mekanizmasını bozarak DDoS etkinliğini gizleyebilir.
- **Hizmet Kesintisinin İtibar ve Regülasyon Riskleri:**
  Tespit edilemeyen veya geç tespit edilen DDoS saldırıları; geniş ölçekli hizmet kesintileri, kritik altyapı güvenliği tartışmaları, regülatif yaptırımlar ve kamuoyu nezdinde güven kaybı ile sonuçlanabilir.
- **AD-GS Bileşenlerinin Hedef Alınması:**
  Saldırganlar, yalnızca şarj yönetim sistemini değil; AD-GS'in kendisini (model sunucuları, izleme ajanları, log toplama altyapısı) hedef alarak tespit mekanizmasını devre dışı bırakmaya çalışabilir; bu da "tekil güvenlik bileşeni"nin kritik bir saldırı yüzeyi hâline gelmesine yol açar.
- **Gizlilik ve Veri Paylaşımı Endişeleri:**
  DDoS tespitine yönelik kapsamlı trafik analizi; kullanıcı davranış profilleri ve konum-temelli kullanım verilerinin işlenmesini gerektirebilir. Bu durum, veri koruma mevzuatı (örn. GDPR uyumu), anonimleştirme ve minimizasyon yükümlülükleri yerine getirilmediğinde hukuki ve etik riskler doğurur.