

# Güç Şebekesi (Siber-Fiziksel) - Sahte Veri Enjeksiyonu (FDI) Saldırısı

## 1. Anomali Tanımı

Şebeke operatörüne (Distribution Network - DN) yönelik sahte yük/voltaj verilerinin enjekte edilmesiyle operatörün yanlış kararlar almasına yol açan saldırılardır. Bu tip saldırılar fiziksel ekipmana zarar verebilir veya dengesizliğe neden olabilir.

## 2. Gözlemler / Tespit Edilecek Belirtiler

- SCADA/EMS'de beklenmedik veri sapmaları ve operatör uyarıları.
- Farklı veri kaynakları (fiziksel sensör vs. telemetri) arasında tutarsızlıklar.

## 3. Tespit Yöntemleri / Teknikler

- Fiziksel-dijital korelasyon: fiziksel sensör verileri ile telemetri arasındaki çapraz doğrulama.
- Anomali tespiti: model tabanlı ve istatistiksel FDI tespit algoritmaları.

## 4. Olası Sebepler / Zafiyetler

- SCADA/telemetri kanallarında doğrulama eksikliği veya zayıf şifreleme.
- Uç cihazlarda güvenlik zafiyetleri ve kimlik doğrulama eksiklikleri.

## 5. Etki / Riskler

- Trafo ve dağıtım ekipmanlarında aşırı yüklenme ve fiziksel hasar.
- Enerji kayıpları, bölgesel kararma ve ekonomik etkiler.

## 6. Önerilen Önlemler / Mitigasyonlar

- Fiziksel sensörlerle çapraz doğrulama ve verilerin kaynağına dayalı güven derecelendirmesi.
- SCADA/EMS kanallarında uçtan uca şifreleme ve mesaj imzalama.
- Anomali tespit sistemleri ve operatör playbook'ları.

## 7. Referanslar

Akıllı dağıtım şebekesi güvenliği literatürü ve FDI tespit makaleleri.