Anomali Araştırması – Fiyat/Fatura Manipülasyonu (OCPP)

Kapsam: Sadece **anomali** bölümünde istenen tüm içeriğin derli-toplu ve detaylı araştırması.
Bağlam: OCPP 1.6J / 2.0.1; CS ↔ CSMS; odak veri akışları: TransactionEvent, MeterValues, Start/StopTransaction, SetVariables/ChangeConfiguration.
Çıktı hedefi: Tespit (detection) yöntemleri, PoC senaryoları, SIEM kuralları, kontrol önlemleri, kabul kriterleri ve artık risk.

---

1) Anomali Tanımı ve Etki

Tanım. OCPP oturum ve ölçüm (meter) verilerinin iletim sırasında yakalanması/değiştirilmesi veya yanlış kaynaklardan üretilmesi sonucu **fiyat/faturalama** bilgilerinin haksız biçimde azaltılması/artırılması.
İş etkisi. Yanlış faturalama, gelir kaybı, müşteri şikâyeti/itibara zarar, yasal uyumsuzluk riski, enerji hırsızlığı.

Manipülasyon örnekleri:

- MeterValues toplam kWh'ın **monotoniklik** ilkesini bozacak şekilde düşmesi/sıfırlanması.
- StopTransaction/TransactionEvent(Ended)'da **süre–enerji** oransızlığı (çok kısa sürede yüksek kWh ya da tersi).
- **Tarife/TOU** parametrelerinin izinsiz değişimi (fiyat çarpanı, zaman dilimi kaydırma).
- **Offline authorization** abuse: cache/list/unknown kipleriyle ücretsiz veya eksik ücretli seans.
- **CS spoofing**: aynı istasyon kimliğiyle birden fazla uç/IP'den eşzamanlı bağlantı.
- **Saat/tarih** manipülasyonu (NTP uyumsuzluğu, saat dilimi/DS kaydırması) ile ücret bandı oynaması.

---

2) İlgili Veri Modeli ve Beklenen Davranış

OCPP 1.6J (örnek alanlar):

- StartTransaction.req: connectorId, idTag, meterStart, timestamp
- StopTransaction.req: transactionId, meterStop, timestamp, transactionData[] (SampledValue dizisi)
- MeterValues.req: transactionId, meterValue[] (her biri timestamp + sampledValue[]), tipik measurand=Energy.Active.Export.Register, unit=kWh

OCPP 2.0.1 (TransactionEvent):

- eventType ∈ {Started, Updated, Ended}, triggerReason, timestamp, transactionInfo (id, chargingState), meterValue (SampledValue[])

Beklenen davranış ilkeleri:

- **Monotoniklik:** Energy.Active.Export.Register ölçümünün oturum boyunca asla azalmaması.
- **Zaman tutarlılığı:** Mesaj zaman damgaları artan sırada; Ended ≥ Started.

- **Fiziksel sınırlar:** Belirli güç (kW) ve süre (saat) için beklenen kWh aralığı.
- **Kimlik tutarlılığı:** transactionId benzersiz ve tek kaynaktan gelir; aynı anda farklı IP'lerden bağlanmaz.

---

3) Saldırı Yüzeyi ve Kök Nedenler

- **Taşıma katmanı zafiyetleri:** ws:// ya da tek taraflı TLS; mTLS'in zorunlu olmaması.
- **Veri bütünlüğü eksikliği:** Sayaç/oturum verilerinde imza/MAC yokluğu → kaynak doğrulama yapılamaz.
- **Konfig kötüye kullanımı (CV):** OfflineTxForUnknownIdEnabled, MaxEnergyOnInvalidId, StopTxOnInvalidId, HeartbeatInterval vb.
- **Kimlik/anahtar yönetimi zafiyetleri:** Sertifika sızıntısı, zayıf depo, rotasyon eksikliği.
- **Saat senkronu eksikliği:** NTP/CA ile yetkili saat kaynağı yok → TOU/Tarife sapması.

---

4) Saldırı Teknikleri (Detay)

1. **MitM + Değer Enjeksiyonu:** TLS yok/yanlışsa MeterValues içindeki SampledValue.value azaltılır ya da ara örnekler düşürülür; MeterStop düşük gösterilir.
2. **Süre–Enerji Kaydırması:** Stop anında süre uzun, kWh artışı düşük (veya tersi) olacak şekilde sahte alanlar yazılır.
3. **Tarife Kaydırma:** Saat dilimi/timestamp manipülasyonu ile pahalı band yerine ucuz banda denk getirme (veya çarpan parametresi oynaması).
4. **Offline Abuse:** CS'yi DoS ile offline düşürüp OfflineTxForUnknownIdEnabled/cache ile yetkisiz kullanım.
5. **CS Spoofing:** Aynı stationId ile sahte uçtan bağlantı kurularak ölçüm/olay sahteciliği.
6. **Precision/Rounding Attack:** resolution/format manipülasyonu ile küçük ama sistematik eksik ölçüm.

---

5) Tespit (Detection) – Kural ve Algoritmalar

K1 – Monotoniklik Kuralı (zorunlu):
Aynı transactionId için sıralı Energy.Active.Export.Register değerleri **azalmamalıdır**.
Formül (ardışık örnekler i<i+1 için): $E[i+1] - E[i] \geq 0 - \varepsilon$
Parametreler: tolerans $\varepsilon \approx 0.01$ kWh (ölçüm/yuvarlama toleransı), pencere: tüm oturum.

K2 – Süre–Enerji Oran Kuralı:
rate = $\Delta kWh / \Delta t$ satıh güç sınırlarıyla uyumlu olmalı.
Alt/üst eşikler: [Pmin, Pmax] → $Pmin * \Delta t \leq \Delta kWh \leq Pmax * \Delta t$.
Not: Pmin ≈ 0.2 kW (beklenen minimum), Pmax kablo/konnektör/konfig limitine göre.

K3 – Zaman Tutarlılığı:
timestamp değerleri artan sırada; Ended.ts ≥ Started.ts. Negatif/ters sıralar **kırmızı bayrak**.

K4 – Kimlik/Network Tutarlılığı:
Aynı stationId için **5 dk içinde ≥2 farklı IP**'den eşzamanlı bağlantı **spoofing** şüphesidir.

K5 – Hızlı CV Değişimi:
15 dk içinde **≥N** kritik CV değişikliği (örn. N=3) → yüksek önemde alarm.

K6 – TLS/mTLS İhlali:
tls_profile < 3 (mTLS değil) ya da client_cert_validation_failed = TRUE → kritik alarm.

K7 – Tarife Bandı Tutarlılığı (opsiyonel):
timestamp → beklenen TOU bandı; faturalama motoru bandıyla uyuşmazsa işaretle.

---

6) SIEM/Sigma Örnekleri (uyarlanabilir)

Monotoniklik (SQL-vari):

```
WITH s AS (
  SELECT transactionId, timestamp, energy_kwh,
       LAG(energy_kwh) OVER (PARTITION BY transactionId ORDER BY timestamp) AS prev
  FROM meter_values
)
SELECT transactionId, timestamp
FROM s
WHERE prev IS NOT NULL AND (energy_kwh < prev - 0.01);
```

Süre–Enerji Oran (KQL-vari):

```
meter_values
| where measurand == 'Energy.Active.Export.Register'
| order by transactionId, timestamp asc
| extend prev_ts = prev(timestamp), prev_kwh = prev(value)
| where isnotempty(prev_ts)
| extend dt = datetime_diff('minute', timestamp, prev_ts) / 60.0,
       dkwh = value - prev_kwh,
       rate = dkwh / dt
| where rate < Pmin or rate > Pmax
```

Hızlı CV Değişimi (Sigma-vari):

```
count_changes_by(cs_id, window=15m, fields=[
```

'OfflineTxForUnknownIdEnabled','StopTxOnInvalidId','MaxEnergyOnInvalidId',

'HeartbeatInterval','SmartChargingEnabled','ExternalControlSignalsEnabled']) >= N

mTLS İhlali:

if (tls_profile < 3) or (client_cert_validation_failed == true) then alert('mTLS violation')

CS Spoofing:

by 5m: count_distinct(ip) by station_id > 1 → alert('CS ID collision')

---

7) PoC / Lab Senaryoları (Sadece Anomali Odaklı)

Ortam: İzole ağ; CSMS sim + CP/CS sim; mitmproxy ile içerik değiştirme; zaman senkronu (NTP).
Araçlar: ocpp, websockets/aiohttp, mitmproxy, log toplayıcı, (opsiyonel) python-can/vcan0.

S1 – Monotoniklik İhlali:

1. Normal seans başlat (StartTransaction/TransactionEvent(Started)).
2. Akışta MeterValues üret.
3. MitM ile E[t+1] ← E[t] - 0.1 değiştir.
4. Beklenen: K1 tetikler; seans faturalama dışına alınır; olay açılır.

S2 – Süre–Enerji Uyumsuzluğu:

1. Seansı düşük güçte sürdür (beklenen ~kwh).
2. StopTransaction/Ended öncesi timestamp ya da kWh değerini orantısız değiştir.
3. Beklenen: K2 tetikler.

S3 – CS Spoofing:

1. Aynı stationId ile ikinci uçtan bağlan.
2. Beklenen: K4 tetikler; eşzamanlı bağlantı kesilir.

S4 – Hızlı CV Değişimi:

1. 15 dk içinde OfflineTxForUnknownIdEnabled, HeartbeatInterval, StopTxOnInvalidId değiştir.
2. Beklenen: K5 tetikler; yüksek önemde alarm.

S5 – mTLS İhlali:

1. ws:// veya TLS1.0/tek-taraflı TLS denemesi yap.
2. Beklenen: K6 tetikler; bağlantı reddi + alarm.

---

8) Kontrol Önlemleri (Anomaliyi Önleme/Azaltma)

- **Taşıma: Security Profile 3 (mTLS)** zorunlu; TLS 1.3; sertifika pinning (mümkünse).

- **Veri bütünlüğü:** TransactionEvent/MeterValues için **imza/MAC**; doğrulama hatasında faturalama dışı bırak.
- **Konfig politikası:** Riskli CV'ler için politika ve iki kişi kuralı; değişimlerin imzalı/versiyonlu kaydı.
- **Saat/NTP:** Yetkili NTP; saat drift ≤ ±1 s; TOU bandı kontrolleri.
- **Anahtar yönetimi:** HSM/SE; sertifika rotasyonu ≤ 12 ay; özel anahtarlar disk düz metin yok.
- **Offline sınırları:** Offline modda enerji/süre/seans sınırı; mümkünse proxy/çift hat ile CSMS sürekliliği.
- **Günlükleme:** Hash-zinciri/izinli defter ile **tamper-evident** log; SIEM entegrasyonu.

---

9) Kabul Kriterleri (Anomali Bölümü İçin)

- **K1–K6** kurallarından **en az biri** manipülasyonu yakalar (Poc S1–S5).
- mTLS devredeyken MitM kaynaklı içerik değişikliği **başarısız** olur veya **iz** bırakır.
- CV kötüye kullanımı belirlenen eşikle **tetiklenir** ve olay kaydı oluşur.
- Yanlış pozitif oranı ≤ %2; algılama gecikmesi ≤ 5 dk.

---

10) Artık Risk ve Yanlış Pozitif Yönetimi

- **Enerji sayacı reset/rollover** nedeniyle görülen doğal düşüşler (donanım reseti) → reset_flag alanı/cihaz günlüğü ile korelasyon.
- **Saat değişimleri/DS** → NTP/TAI referansı ve tekil zaman çizgisi kullanımı.
- **Düşük güç profilleri** → Pmin'i konnektör/araç tipine göre dinamik ayarlama.
- **EV vs EVSE sayaç ayrımı** → hangi kaynağın faturalandığı net; çift taraflı doğrulama mümkünse.

---

11) Örnek OCPP Mesaj Fragmanları

1.6J – MeterValues.req (özet):


```
{
 "connectorId":1,
 "transactionId": 5421,
 "meterValue":[{
  "timestamp":"2025-11-07T21:11:00Z",
  "sampledValue":[{"measurand":"Energy.Active.Export.Register","unit":"kWh","value":"12.35"}]
 }]
```

}

2.0.1 – TransactionEvent (Updated):

{

"eventType":"Updated",

"timestamp":"2025-11-07T21:12:00Z",

"transactionInfo":{"transactionId":"abc-123"},

"meterValue":[{"sampledValue":[{"measurand":"Energy.Active.Export.Register","unit":"kWh","value":"12.47"}]}]

}

Manipüle örnek (monotoniklik bozan): value: "12.45" → "12.40" (K1 tetikler).

---

12) İzlenecek CV'ler (Hızlı Liste)

SecurityProfile, AuthorityPublicKey, BasicAuthPassword (devre dışı), HeartbeatInterval, MessageTimeout, Retry*, OfflineTxForUnknownIdEnabled, StopTxOnInvalidId, MaxEnergyOnInvalidId, SmartChargingEnabled, ExternalControlSignalsEnabled, ClockAlignedDataInterval.

---

13) Uygulama Notları

- SIEM'de **transactionId** ve **stationId** kimliklerini birleştirip pencere bazlı korelasyon kurun.
- Faturalama motoruna **anormallik bayrağı** aktarın; manuel inceleme kuyruğu.
- Test verileri için **senaryolaştırılmış JSON** ve **ekran görüntüleri** toplayın; rapora ekleyin.