Codenight Case: Turkcell TrustShield – Şüpheli İşlem ve Risk Case Yönetimi Platformu

Amaç

Ekipler, Turkcell servislerinden gelen kullanıcı olaylarını (Paycell, BiP, Superonline, TV+) bir araya getirerek **risk sinyalleri üreten**, bu sinyallere göre **aksiyon alan** ve gerektiğinde **fraud case (inceleme kaydı)** açıp yöneten bir sistem geliştirir.

Sistem; gelen olayları işler, risk kurallarını uygular, aksiyon üretir ve kararlarını kayıt altına alır.

Temel Özellikler

1. Olay (Event) Yönetimi

- Sistem, servislerden gelen verileri **event** olarak işler.
- Her event şu alanları içermelidir:
    - kullanıcı
    - servis
    - event türü
    - değer
    - zaman bilgisi
    - opsiyonel meta alanı (ör. cihaz, ip risk, merchant)

Örnek event:


```
{
  "event_id": "EV-5002",
  "user_id": "U5",
  "service": "Paycell",
  "event_type": "PAYMENT",
  "value": 950,
  "unit": "TRY",
  "meta": "merchant=CryptoExchange",
  "timestamp": "2026-03-12T19:06:00Z"
```

}

---

2. Risk Profili (Risk Profile / State)

- Sistem her kullanıcı için güncel bir **risk profili** tutmalıdır.
- Risk profili aşağıdaki gibi alanlar içerebilir:
    - risk_score (0–100)
    - risk_level (LOW/MEDIUM/HIGH)
    - signals (hangi sinyaller oluştu)

Örnek:

{

"user_id": "U5",

"risk_score": 90,

"risk_level": "HIGH",

"signals": ["high_ip_risk_new_device", "crypto_payment"]

}

---

3. Risk Kural Motoru

- Risk değerlendirmesi için **veri bazlı (data-driven) kurallar** uygulanmalıdır.
- Kurallar kod içine gömülmemeli, veri olarak yönetilebilir olmalıdır.

Örnek kural:

{

"rule_id": "RR-01",

"condition": "BiP yeni cihaz + ip_risk=high",

"action": "FORCE_2FA",

"priority": 1,

"is_active": true

}

Bir kullanıcı için aynı anda birden fazla kural tetiklenebilir.

---

4. Aksiyon Yönetimi

- Kurallar sonucunda bir veya daha fazla aksiyon oluşabilir.
- Örnek aksiyonlar:
    - FORCE_2FA (ek doğrulama zorunlu)
    - PAYMENT_REVIEW (işlem incelemeye düşsün)
    - TEMPORARY_BLOCK (geçici blok)
    - OPEN_FRAUD_CASE (inceleme kaydı aç)

Birden fazla aksiyon oluştuğunda:

- Öncelik değerine göre seçim yapılmalı
- Seçilmeyen aksiyonlar bastırılmalı veya kayda alınmalı

---

5. Fraud Case Yönetimi

- Belirli aksiyonlar bir **case (inceleme kaydı)** oluşturmalıdır.
- Case alanları:
    - case_type
    - status (OPEN / IN_PROGRESS / CLOSED)
    - priority (LOW/MEDIUM/HIGH/CRITICAL)
    - opened_at
- Case üzerinde aksiyon geçmişi tutulmalıdır (audit trail).

---

6. Bildirim (BiP Mock)

- Seçilen aksiyonların kullanıcıya BiP üzerinden bildirimi yapılmalıdır (mock).

Örnek:

{

"user_id": "U5",

"message": "Güvenlik nedeniyle ek doğrulama (2FA) zorunlu hale getirildi."

}

---

7. Karar ve Kayıt (Audit Log)

- Sistem, her karar için aşağıdaki bilgileri kaydetmelidir:
    - tetiklenen kurallar
    - seçilen aksiyon
    - bastırılan aksiyonlar
    - zaman bilgisi

Örnek:

{

"decision_id": "D-2003",

"user_id": "U5",

"triggered_rules": ["RR-01", "RR-02"],

"selected_action": "FORCE_2FA",

"suppressed_actions": ["PAYMENT_REVIEW"],

"timestamp": "2026-03-12T19:09:00Z"

}

---

8. Yönetim ve İzleme Ekranı (Dashboard)

Dashboard'da aşağıdakiler yer almalıdır:

- Son gelen event'ler
- Kullanıcı risk seviyeleri ve skorları
- Açık fraud case'ler ve durumları

- Tetiklenen kurallar ve aksiyonlar
- Karar logları

Dashboard web tabanlı olabilir; mobil uyum zorunlu değildir.

Bonus Özellik: Risk Rule Yönetim Ekranı (Opsiyonel)

Sistem içinde risk kurallarının arayüz üzerinden yönetilebildiği bir ekran geliştirilmesi beklenir.

Beklenenler:

- Kural listeleme (rule_id, condition, action, priority, is_active)
- Kural ekleme / güncelleme
- Kural aktif/pasif yapabilme
- Değişikliklerin kaydedilmesi ve motorun güncel kurallarla çalışması

Veri Modeli (CSV / JSON)

users
user_id, name, city, segment

events
event_id, user_id, service, event_type, value, unit, meta, timestamp

risk_rules
rule_id, condition, action, priority, is_active

risk_profiles
user_id, risk_score, risk_level, signals

fraud_cases
case_id, user_id, opened_by, case_type, status, opened_at, priority

case_actions
action_id, case_id, action_type, actor, note, timestamp

decisions
decision_id, user_id, triggered_rules, selected_action, suppressed_actions, timestamp

bip_notifications
notification_id, user_id, channel, message, sent_at

API Önerisi

POST /events

GET /users/{id}/risk-profile

GET /risk-rules

POST /risk-rules

PUT /risk-rules/{rule_id}

GET /fraud-cases

GET /decisions

GET /dashboard/summary

Puanlama Kriterleri (Genel – 100 Puan)

Kategori	Puan
Temel İşlevsellik ve Doğru Çalışma	30
Veri Modeli ve Sistem Tasarımı	20
Kural ve Karar Mekanizması	20
Kod Kalitesi ve Yapı	15
Görsellik ve Anlatılabilirlik	10
Bonus Özellikler	5