



PRD – AI Tabanlı Log Analizi Yazılımı

Ürün Bilgileri

Ürün Adı (çalışma adı): Akıllı Log Asistanı

Tarih: 24 Temmuz 2025

Sürüm: MVP v1.0

1. Ürün Özeti ve Vizyonu

Bu ürün, sistem yöneticilerinin altyapı loglarını manuel analiz etme yükünü ortadan kaldırarak, AI destekli otomatik anomali tespiti ve uyarı sistemi sunar. Dağıtık sistemlerden gelen büyük boyutlu logları analiz ederek sistem güvenliği ve operasyonel verimliliği artırmayı hedefler.



Vizyon: IT ekiplerine, logların arasında kaybolmadan erken uyarılarla sistem güvenliğini proaktif yönetebilecekleri bir araç sunmak.

2. Hedefler ve Başarı Metrikleri

- MVP bugün yayınlanacak
- Kullanıcı hedefi: 1 sistem yöneticisi (pilot kullanıcı)
- Model doğruluğu \geq %95
- Yanlış pozitif oranı \leq %5
- Kritik hata uyarı süresi \leq 5 saniye

3. Kullanıcı Tanımları ve Senaryolar






Hedef Kullanıcı:

- Bir sistem yöneticisi
- Kurum içi loglara erişimi var
- Teknik bilgiye sahip ancak AI konusunda uzman değil


Kullanıcı Hikayesi:

"Bir sistem yöneticisi olarak, loglarda oluşan beklenmeyen davranışları manuel olarak incelemek yerine, otomatik tespit ve uyarı almak isterim. Böylece zaman kaybetmeden kritik olaylara odaklanabilirim."

4. Temel Özellikler (MVP v1.0)

Özellik	Açıklama
 Log Yükleme	Kullanıcı, CSV veya .log formatında dosya yükleyebilecek
 AI Tabanlı Anomali Tespiti	Loglar basit bir modelle analiz edilip anomali varsa işaretlenecek
 Anomali Görselleştirme	Tespit edilen anomali kayıtları listelenecek ve renklendirilecek . AI kullanarak(Tehlikenin türü, tablolaştırılması,daha kullanıcı dostu bir arayüz), daha anlaşılır olsun
 Basit Bildirim	Web arayüzü üzerinden "kritik anomali" bildirimi gösterilecek
 Log Arama	Loglar tarih/satır/anahtar kelime ile filtrelenebilecek

5. AI ve Veri Gereksinimleri

- **Model Tipi:** RandomForestClassifier + TF-IDF (klasik ML, hızlı eğitim)
- **Öznitelikler:** Satır uzunluğu, büyük harf kullanımı, özel karakter oranı, tarih/port/IP içeriği, TF-IDF metin vektörü
- **Veri Kaynağı:**
 - LogPai - BGL Dataset (Berkeley) 



- HDFS log_dataset (Huawei)
 - **Model Cevap Süresi:** ≤ 1 saniye
 - **Veri Saklama:** 30 gün (varsayılan), log ID üzerinden anonimleştirme yapılabilir
 - **Gizlilik:** IP adresi, kullanıcı adı gibi PII öğeleri maskeleyen filtrelerle sansürlenecek
-

6. İşlevsel & Teknik Gereksinimler

Fonksiyonel Gereksinimler:

- Giriş yapılmadan kullanılabilen tek-kullanıcı web arayüz
- Log dosyası yükleme alanı (.csv, .log)
- Log örneklerini listeleme
- AI modelini çalıştırıp anomali tespiti sunma

Teknik Gereksinimler:

- **Veritabanı:** SQLite (tek kullanıcı için yeterli)
 - **Backend:** FastAPI (Python tabanlı)
 - **Frontend:** React + Shadcn/ui (sade ve erişilebilir)
 - **UI Kit Önerisi:**  shadcn/ui — Tailwind tabanlı, sade, komponent odaklı
 - **Dağıtım:**
 -  **Docker Compose** (çünkü kurum içi ve offline çalışma isteniyor)
 - Gerekirse nginx reverse proxy eklenebilir
 - **Log format desteği:** CSV (öncelik), JSON (opsiyonel)
-

7. Kullanıcı Akışları

Kullanıcı Akışı: Anomali Tespiti

markdown

KopyalaDüzenle

1. Log dosyası yüklenir (.csv)
2. Kullanıcı "Analizi Başlat"a tıklar
3. Sistem logu işler, AI modeliyle anomalileri etiketler
4. Kritik seviyeli satırlar renkle vurgulanır
5. Kullanıcı filtreleme/arama ile detay inceler

8. Riskler ve Varsayımlar



Riskler:

- Modelin çok fazla yanlış pozitif üretmesi (özellikle kısa loglarda)
- Log formatlarının yükleme sırasında bozulması (örneğin encoding hataları)



Varsayımlar:

- Kullanıcı kurum içi ağı kullanıyor
- Dış bağlantı (internet) olmayabilir → model, arayüz ve analiz tamamen local çalışmalı
- Kullanıcılar teknik kavramları temel düzeyde anlayabiliyor

9. Kabul Kriterleri

Özellik	Kabul Kriteri
Log Yükleme	Sistem, max 50MB'lık log dosyasını 5 saniyeden kısa sürede yüklemeli
Anomali Tespiti	Tespit edilen satırların listesi görüntülenebilmeli, kritik olanlar kırmızı vurgulu olmalı
Performans	Ortalama analiz süresi < 2 saniye
Uyarı Sistemi	Web arayüzünde anomali bildirimi modal ya da toast olarak görünmeli

10. UI/UX Beklentileri

- Minimal, bileşen odaklı arayüz → **Shadcn/ui** kullanılacak
 - Karanlık tema desteği
 - 2-3 tıklama ile tüm işlemler tamamlanabilir olmalı
 - Anomaliler renkli rozetlerle (badge) vurgulanmalı
 - Log tabloları sortable & filtrelenebilir olmalı
 - Kullanıcı dosya yüklerken durum göstergesi almalı (progress bar)
-

11. Kısıtlar ve Uyumluluk

- **Dağıtım:** Kurum içi, Docker tabanlı
 - **Ağ:** Offline mod desteği (tüm bileşenler yerel çalışmalı)
 - **Yasal Uyumluluk:** Kullanıcı verisi anonimleştirilmeli
 - **Zaman:** İlk MVP sürümü 24 Temmuz 2025 itibarıyla tamamlanmalı
 - **Kısıtlama:** Sadece tek kullanıcı destekleniyor (demo ortamı)
-

Sonuç & Devam

PRD tamamlandı. İstersen:

- Markdown veya PDF olarak çıktı alabiliriz
- Teknik ekip için `README.md` veya kurulum dokümanı yazabilirim
- Gerekirse proje klasör yapısını ve ilk dosyaları çıkarabiliriz