

Web Sitesi İzlenebilirlik (Log/Metric/RUM) Planlama Şablonu — Yazılım / Observability (v1.0)

Asset Amaç: Bu şablon, kurumsal web siteleri ve dijital platformlar için altyapısal Log–Metric–Trace üçlüsünü, son kullanıcı deneyimini anlık ölçen RUM (Real User Monitoring - Core Web Vitals/JS hataları) katmanı ile tek bir bütünlük gözlemlenebilirlik (observability) modelinde planlamanızı sağlar. Otel rezervasyon motorları ve B2B kurumsal portalları gibi kritik kullanıcı akışları için gösterge panellerini (dashboard) ve alarm eşiklerini "alarm yorgunluğu" yaratmayacak, doğrudan aksiyon alıracak biçimde kurgular. Ayrıca log güvenliği (PII maskeleyme) ve acil durum müdahale (runbook) yaklaşımıyla sistemlerin operasyonel sürdürülebilirliğini ve yasal uyumluluğunu hedefler.

Kim Kullanır?: Teknik Liderler (Tech Lead), DevOps / SRE Mühendisleri, Ön Yüz Yazılım Liderleri (Frontend Lead), Analitik ve Raporlama Sorumluları ile Ürün Sahipleri (Product Owner).

Nasıl Kullanılır?

- Platformunuz üzerindeki en kritik kullanıcı görevlerini (user tasks) ve sistem modüllerini (rezervasyon adımları, form gönderimleri, B2B rapor çıktıları) öncelik sırasına göre listeleyin.
- Belirlediğiniz her ana görev için toplanacak log, metrik ve RUM sinyallerini eşleştirerek, sistemin kırmızı alarmı geçeceği eşik değerlerini dokümana işleyin.
- Canlıya alım (go-live) ve sürüm (release) sonrası izleme rutinlerini netleştirip, olası bir kesinti anında ilk 10 dakikada uygulanacak kriz müdahale planını (incident runbook) hayata geçirin.

TEMPLATE — Web Sitesi İzlenebilirlik (Log/Metric/RUM) Planlama Şablonu

A) Boş Şablon Alanları (Observability Matrisi)

1) Kritik Kullanıcı Görevleri (User Tasks)

Sistem genelinde izlenecek, iş modelinin kalbini oluşturan kritik akış tanımları:

- Otel Grubu Senaryoları (Örn: Rezervasyon Başlatma, Oda Seçimi, Ödeme Geçidi):** _____
- B2B Portalı Senaryoları (Örn: Cari Dashboard Açılışı, Excel/Rapor Export Süreçleri):** _____
- Ortak Platform Akışları (Örn: Kullanıcı Girişi / Login, İletişim & Lead Formu Gönderimi):** _____

2) Gözlemlenebilirlik Sinyal Haritası

Kullanıcı görevlerinin teknik olarak hangi katmanlardan izleneceğini gösteren merkezi matris:

 **Observability Sinyal Dağılım Matrisi (image_e5e1a7.png)**

Kritik Görev (Task)	Log Sinyalleri	Metrik & Trace	RUM Sinyalleri (Real User)
Ödeme / Form Akışı	_____	_____	_____
Dashboard / Rapor	_____	_____	_____
Giriş / Login	_____	_____	_____

3) Alarm Eşikleri ve Kırmızı Çizgiler (Alerting Thresholds)

Sistemin anormallik durumlarında otomatik slack, sms veya pagerduty uyarısı fırlatacağı sınır değerleri:

- **5xx Sunucu Hata Oranı (5xx Error Rate):** [] Toplam trafiğin %____ değerini aşması durumunda
- **Yanıt Gecikme Süresi (p95 Latency):** [] Yanıt süresinin ____ ms değerinin üzerine çıkması durumunda
- **JavaScript Hata Sıçramaları (JS Error Spike):** [] Tarayıcı anlık hata hacminin %____ artması durumunda
- **Core Web Vitals Performans Bozulması:** [] LCP / INP değerinin ____ saniye baremini aşması durumunda
- **İşlemsel Kayıp Sinyali (Drop-off Spike):** [] Dönüşüm hunisinde anlık %____ oranında ani kopma yaşandığında

4) Dashboard (Gösterge Paneli) Mimari Seti

Operasyonel durumu ve iş sağlığını anlık izlemek için kurulacak 3 katmanlı ekran kurgusu:

- **Business Health Dashboard (İş Sağlığı):** Canlı rezervasyon adetleri, başarılı B2B form hacimleri ve dönüşüm oranları izleme alanı.
- **Ops Health Dashboard (Altın Sinyaller):** Trafik (Saturate), Hata Oranı (Errors), Gecikme (Latency) ve Dağıtım (Concurrency) takibi.
- **Debug & Trace Dashboard (Derinlemesine Analiz):** Hata kodlarının kök nedenini bulmayı sağlayan uçtan uca trace izleme alanı.

5) Log Güvenliği ve Veri Gizliliği (Compliance)

Log sistemlerine sızabilecek hassas verilerin KVKK ve güvenlik politikalarına göre korunması:

- **PII (Kişisel Veri) Maskeleye Kuralları:** Kredi Kartı / Telefon / E-posta / Şifre alanlarının regex ile maskelenmesi
 - **Log Saklama Süresi (Retention Policy):** Hot Storage: ____ Gün / Cold Archive: ____ Gün
 - **Rol Bazlı Log Erişim Yetkilendirmesi (RBAC):**
-
-

6) Incident Runbook (Kesinti Anında İlk 10 Dakika Aksiyon Planı)

Sistem alarm verdiğinde nöbetçi mühendisin izleyeceği standart operasyon adımları:

- **1. Aşama - Durum Değerlendirmesi (Triage):** Hatanın kapsamını ve etkilenen kullanıcı sayısını anlama adımları: _____
- **2. Aşama - Geçici Çözüm / Azaltma (Mitigation):** Sistemi hızla ayağa kaldırma yöntemi: Otomatik Rollback / Trafik Yönlendirme
- **3. Aşama - Doğrulama (Verify):** Uygulanan çözümün hatayı bitirip bitirmediğini test etme kriteri: _____
- **4. Aşama - Kalıcı Çözüm Dokümantasyonu (Postmortem):** Kök neden analizi ve geleceğe yönelik önlem toplantı takvimi: _____

B) Nasıl Doldurulur? (5 Kritik Kural)

1. **"Her Şeyi İzleyelim" Tuzağından Kaçının:** Altyapıdaki tüm önemsiz logları ve sistem metriklerini izleyip dashboard'ları çöplüğe çevirmeyin. Sadece iş modelini ayakta tutan kritik kullanıcı görevlerine (rezervasyon, ödeme, üyelik) odaklanarak işe başlayın.
2. **Alarm Sayısını Sınırlayın ve Net Owner Atayın:** Sık sık çalan ama kimsenin dönüp bakmadığı anlamsız alarmlar oluşturmayın (alarm fatigue). Kurulan her alarm eşliğinin tetiklendiğinde hangi mühendise düşeceği ve o an hangi aksiyonun alınacağı önceden dokümanate edilmiş olmalıdır.
3. **Teknik İzlemeye Mutlaka RUM Katmanını Ekleyin:** Sunucularınızın %100 ayakta olması (uptime) sitenin sağlıklı çalıştığı anlamına gelmez. Kullanıcının tarayıcısındaki şişmeleri, Core Web Vitals (CWV) düşüşlerini ve JS arayüz çökmelerini yakalamak adına Real User Monitoring sistemlerini mutlaka devreye alın.
4. **Hassas Verileri Loglara Sızdırmayın:** Kullanıcıların e-posta, telefon veya şifre gibi PII (Kişisel Veri) niteliğindeki bilgilerini loglama araçlarına ham metin (plain text) olarak kesinlikle basmayın; front-end ve back-end katmanlarında regex maskeleye filtreleri kurun.
5. **Her Sürüm (Release) Sonrası 60 Dakikalık Gözlem Penceresi Açın:** Yeni bir kod canlıya alındıktan sonraki ilk bir saati resmi izleme dönemi ilan edin. Geliştirici ekip dashboard başında hata sıçramalarını (spikes) gözlemeden işi "bitti" kabul etmemelidir.

C) Doldurulmuş 1 Pratik Örnek (Kısa Senaryo)

- **Seçilen Kritik Kullanıcı Görevi:** Otel web sitesi ve rezervasyon motorundaki "Kredi Kartı ile Ödeme" adımı.
- **Log Sinyali Kurgusu:** Sistem `payment_success`, `payment_error_code_3002` (bakiye yetersiz) ve `provider_gateway_timeout` loglarını basmaktadır.

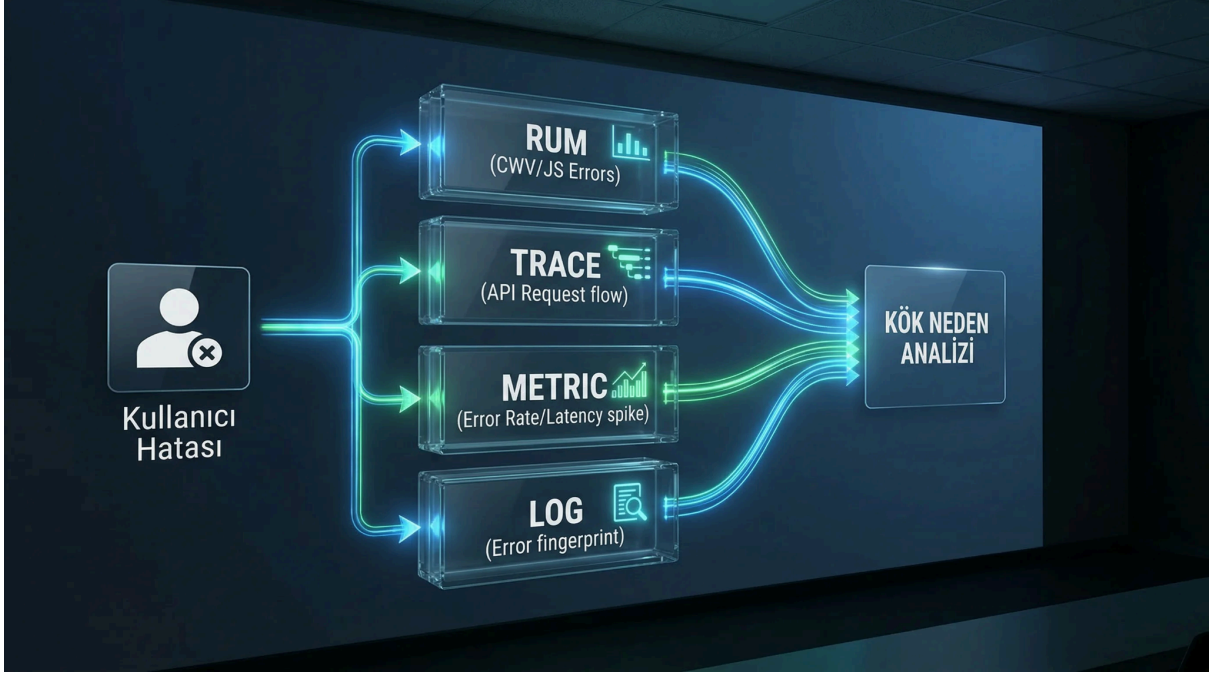
- **Metrik & RUM Entegrasyonu:** Sunucu tarafında p95 yanıt gecikmesi 800ms altında tutulurken, tarayıcı tarafında (RUM) ödeme butonuna tıkladığında oluşan anlık JS error spike metrikleri ve kullanıcı drop-off (sayfadan kaçma) oranları anlık izlenmektedir.
- **Otomatik Alarm Davranışı:** Ödeme sayfasındaki 5xx sunucu hata oranı son 5 dakikada %2 barajını aşarsa veya kullanıcıların ödeme adımından ani kopma (drop) oranı %15 artarsa sistem nöbetçi SRE mühendisine "Kritik Seviye" PagerDuty çağrısı fırlatır ve anında rollback runbook'u tetiklenir.

D) Teknik Kontrol Listesi (Checklist)

- [] **Görevler Belirlendi:** Platformun iş sağlığını belirleyen tüm kritik kullanıcı akışları ve görevleri dökümantasyona işlendi.
- [] **Bütünleşik İzleme Aktif:** Belirlenen akışlar için Log, Metric ve RUM (Real User) sinyal haritalama matrisi dolduruldu.
- [] **Aksiyonel Alarmlar Hazır:** Alarm yorgunluğunu önleyecek net alarm eşik değerleri atandı ve operasyonel sahipleri (owner) seçildi.
- [] **3 Katmanlı Panel Kuruldu:** Business, Ops ve Debug süreçlerine özel ayrı gösterge paneli (dashboard) tasarımları tanımlandı.
- [] **KVKK & Log Güvenliği Tamam:** Log havuzuna düşecek PII verilerinin maskelenme kuralları, yetki (RBAC) ve silinme (retention) süreleri yazıldı.
- [] **Kriz Planı Devrede:** Acil durumlar için ilk 10 dakikalık müdahale runbook adımları ve canlı sürüm sonrası 60 dakikalık gözlem ritmi süreçleştirildi.

Deliverables (Teslim Edilecek Çıktılar)

- Teknik Ekipler İçin 1 Adet Entegre Gözlemlenebilirlik (Observability) Sinyal Haritası Dokümanı
- Kesinti Sürelerini (MTTR) Kısaltan 1 Adet Net Alarm Eşikleri ve Kriz Müdahale Runbook Planı
- DevOps ve SRE Takımlarına İletilecek 1 Adet 3 Katmanlı Dashboard Tasarım Şablonları Paketi



[Architecture Gözlemlenebilirlik Diagram]

Modern bir web uygulamasının bütünleşik izleme mimarisini açıklayan, 16:9 formatında çizilmiş teknik bir gözlemlenebilirlik (observability) diyagramı. Gece siyahı arka plan üzerinde, sol tarafta kullanıcının tarayıcısından (RUM katmanı) yükselen Core Web Vitals ve JS hata verileri parlıyor. Bu veriler ortada birleşerek, uygulamanın iç dünyasından gelen Altyapı Metrikleri (Metrics), Sistem Günlükleri (Logs) ve Uçtan Uca Takip (Distributed Tracing) sinyalleriyle harmanlanıyor. Tüm bu veri akışının merkezi bir akıllı analiz motoruna nasıl aktığı, net neon mavi ve mor renk kodlu çizgilerle scannable bir şekilde şemalaştırılıyor.



[Observability Dashboard Mockup]

Sistem mühendisleri ve ürün sahiplerinin kriz anlarında veya günlük operasyonlarda durum kontrolü yapabilecekleri, 16:9 formatında tasarlanmış minimalist bir izleme paneli (dashboard) mockup görseli. Mat antrasit zemin üzerinde, sol üst köşede parlayan neon yeşili hatlarla başarılı rezervasyon/dönüşüm grafikleri (Business Health), sağ üst köşede p95 gecikme sürelerini gösteren mavi çizgi grafikler (Ops Health) yer alıyor. Alt yarımda ise olası bir JavaScript veya 5xx hatası fırladığında anında devreye giren parlayan kırmızı bir alarm kartı ("JS Error Spike Detected - Action Required") ve nöbetçi ekibe atanan aksiyon butonları sergilenerek tam bir süreç okunabilirliği sunuluyor.