Altyapı Monitoring & Incident Management Checklist Şablonu — Yazılım / Sunucu ve Güvenlik (v1.0)

Asset Amaç: Bu asset; izleme (*monitoring*) mekanizmalarını sağlık (health), performans (performance) ve güvenlik (security) katmanlarında bütünsel kurgulayıp olay yönetimi (*incident management*) süreçleriyle (on-call rotaları, müdahale protokolleri ve postmortem analizleri) birleştirmek için hazırlanmıştır. SSL sertifikası veya domain süresinin dolması gibi "tamamen önlenebilir" kesintileri sıfıra indirmeyi, kaynak yetersizliği (*capacity*) ve anomali durumlarını kriz dönüşmeden erken yakalamayı hedeflemeyi amaçlar. Üretilen alarmları doğrudan iş etkisi (*business impact*) raporlamasıyla ilişkilendirir.

Kim Kullanır?: DevOps / SRE Mühendisleri, Sistem Yöneticileri, Otel / B2B Operasyon Liderleri.

Nasıl Kullanılır?

1. Kritik iş akışlarınızı (*rezervasyon, portal, veri aktarımı vb.*) listeleyip "Golden Signals" (Latency, Traffic, Errors, Saturation) setini tanımlayın.
2. Alarm eşiklerini yapılandırarak On-Call nöbet ve eskalasyon mekanizmasına bağlayın.
3. Olay sonrası Blameless Postmortem şablonunu uygulayın ve tespit edilen kök nedenleri sürekli iyileştirme backlog'una aktarın.

CHECKLIST & SPRINT PLAN — Altyapı Monitoring & Incident Management

1) Ölçüm & Önceliklendirme Kontrol Listesi (Checklist)

- [ ] **Health (Uptime) Kontrolleri:** HTTP(S), DNS, TCP Port ve ICMP check'leri dış ağdan periyodik olarak çalışıyor.
- [ ] **Perf (Performans) Kontrolleri:** p95/p99 gecikme süreleri (*latency*) ve HTTP 5xx hata oranları gerçek zamanlı izleniyor.
- [ ] **Capacity (Kapasite) Kontrolleri:** CPU, RAM, Disk I/O ve Network Bandwidth için kalan alan (*headroom*) ve doluluk eşikleri takip ediliyor.
- [ ] **SSL Expiry Alarmları:** Sertifika bitiş tarihine 30, 14 ve 7 gün kala otomatik uyarı üreten katmanlı alarmlar aktif.
- [ ] **Domain Expiry Alarmları:** Alan adı yenileme zamanı için DNS/Whois takip alarmı kurgulandı.
- [ ] **Anomali & Güvenlik Sinyalleri:** Anormal trafik artışları, WAF engellemeleri ve şüpheli/başarısız giriş denemeleri izleniyor.
- [ ] **Kuyruk & İşlem Alarmları:** Arka plan iş kuyrukları (*Queue Depth / Worker Delay*) ve veri aktarım hatası uyarıları tanımlı.
- [ ] **On-Call & Eskalasyon Yapısı:** Nöbetçi mühendis rotası ve yanıtsız kalan kritik alarmlar için eskalasyon zinciri netleştirildi.
- [ ] **Erişilebilir Runbook'lar:** Her kritik alarm için müdahale adımlarını içeren standart çalıştırma rehberleri (*runbook*) güncel.

- [ ] **Postmortem Süreci & Aksiyon Takibi:** Kesinti sonrası kök neden analizi (RCA) ve kriz son bildirim süreci tanımlandı.

2) Problem → Kök Neden → Çözüm Tablosu

Problem	Kök Neden	Çözüm (Incident Ops)
Kullanıcı Şikâyetiyle Fark Etme	Proaktif izleme ve alarm mekanizmasının olmaması	**Golden Signals** (Latency, Traffic, Errors, Saturation) $\mathbf{+}$ Alerting
Sertifika Bitti / Kesinti Oluştu	SSL/Domain süre takibinin otomatize edilmemesi	**30/14/7 Gün Kademeli Alarm** $\mathbf{+}$ Auto-Renew Süreci
Alarm Gürültüsü / Yanlış Alarmlar	Hatalı veya fazla hassas alarm eşik ayarları	**Alarm Kalibrasyonu** $\mathbf{+}$ Geçici Bastırma (*Suppress*) Kuralları
Tekrarlayan Olaylar ve Kesintiler	Olay sonrası kök neden analizinin yapılmaması	**Blameless Postmortem** $\mathbf{+}$ Düzeltici Aksiyon Backlog'u

3) 14 Günlük Uygulama Sprint Planı (Gün 1–14)

[Gün 1–5: Metrik & Dashboard] ⟶ [Gün 6–10: Alarm & On-Call Triage] ⟶ [Gün 11–12: Postmortem & Etki] ⟶ [Gün 13–14: Tatbikat & Backlog]

- **Gün 1:** Kritik iş akışlarının envanterinin çıkarılması (Rezervasyon motoru, B2B portalı, veri aktarım hatları).
- **Gün 2:** Golden Signals setinin tanımlanması (Gecikme, Trafik, Hata, Doygunluk).
- **Gün 3:** Uptime kontrollerinin (HTTP, DNS, Port) dış izleme servislerinde kurgulanması.
- **Gün 4:** Performans izleme panellerinin (p95 latency, HTTP 5xx, TTFB) oluşturulması.
- **Gün 5:** Kapasite izleme panellerinin (CPU, RAM, Disk doluluğu) hazırlanması.
- **Gün 6:** SSL ve Domain geçerlilik süresi (Expiry) alarmlarının kurulması.
- **Gün 7:** Kuyruk derinliği (Queue Depth) ve güvenlik/trafik anomali alarmlarının tanımlanması.
- **Gün 8:** On-Call nöbet rotasının ve eskalasyon zincirinin (PagerDuty / Opsgenie / Slack) yapılandırılması.

- **Gün 9:** Olay müdahale şablonlarının (*Triage*) ve ilk müdahale rehberlerinin (*Runbook*) hazırlanması.
- **Gün 10:** Yanlış alarmların temizlenmesi, eşik değerlerinin kalibre edilmesi (*Alarm Noise Reduction*).
- **Gün 11:** Olay sonrası analiz (*Blameless Postmortem*) şablonunun oluşturulması.
- **Gün 12:** Alarmların iş etkisi (*Business Impact*) ve finansal risk metrikleriyle ilişkilendirilmesi.
- **Gün 13:** Masabaşı olay simülasyonu / kriz tatbikatı (*Tabletop Incident Simulation*) yapılması.
- **Gün 14:** Yönetim özet raporunun hazırlanması ve sürekli iyileştirme backlog'unun kilitlenmesi.

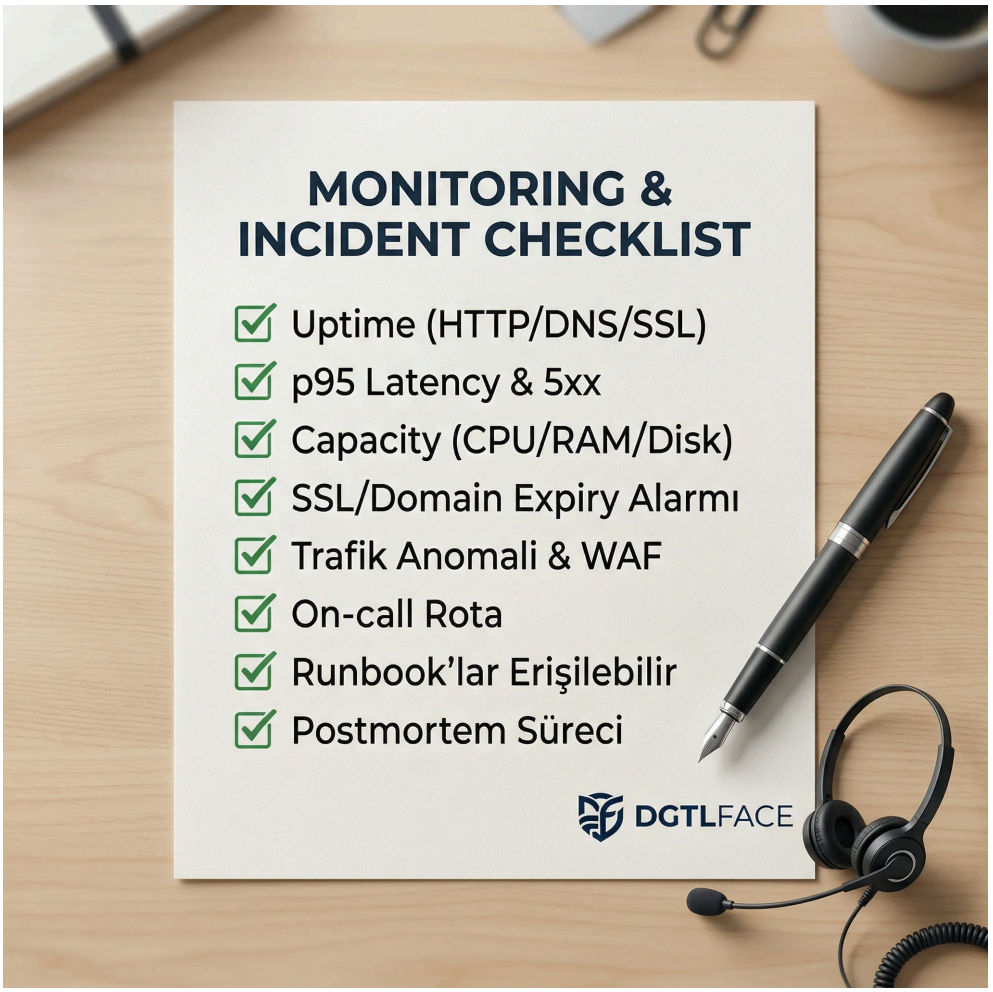
4) Öncesi / Sonrası KPI Tablosu

KPI Metriği	**Önce (Mevcut Durum)**	**Sonra (Sprint Sonrası)**	**Hedef Yönü**
MTTR (Mean Time to Resolve)	$\sim 180\text{ dk}$	$< 25\text{ dk}$	**Hedef $\downarrow$ (Düşüş)**
Uptime (Sistem Kullanılabilirliği)	$\%98.5$	$\%99.9+$	**Hedef $\uparrow$ (Yükselme)**
SSL / Domain Expiry Incident	Yılda 2–3 Olay	0 (Sıfır Olay)	**Hedef 0 (Sıfırlama)**
Alarm Gürültüsü (False Positive)	Yüksek	Minimum (Kalibre Edilmiş)	**Hedef $\downarrow$ (Düşüş)**

Deliverables (Teslim Edilecek Çıktılar)

- **Bütünsel İzleme Dashboard Seti (v1.0):** Health, Performance, Capacity ve Security panelleri (Grafana/Datadog uyumlu).
- **Alarm Kural Seti & Standart Runbook Dokümantasyonu:** Kritik alarmların tanımı, eşik değerleri ve müdahale adımları kılavuzu.
- **On-Call Nöbet Rotası & Triage Müdahale Şablonu:** Nöbet değişimi, olay sınıflandırma ve iletişim kuralları rehberi.

- **Blameless Postmortem Şablonu & İyileştirme Backlog'u:** Olay sonrası kök neden analizi ve önleyici aksiyon takip formu.



[Checklist Card]

DevOps mühendisleri, SRE'ler ve altyapı operasyon liderleri için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Monitoring & Incident Management Checklist Kartı. Koyu karbon gri ve parlak turuncu/kırmızı/siyan tonlarındaki teknolojik zemin üzerinde; canlı metrik grafikleri, SSL ve uptime uyarı ikonu, On-Call nöbet akış şeması ve 14 günlük incident ops sprint takvimi yer alıyor. Kartın üzerinde; "Golden Signals & Capacity Monitoring Dashboards", "Proactive SSL & Domain Expiry Alerting", "On-Call Rotations & Incident Triage Runbooks" ve "Blameless Postmortem & Action Backlog Tracking" teslimat kalemi başlıkları, yanlarında parlak turuncu onay işaretleriyle scannable ve kurumsal bir checklist-card formatında sergileniyor.