Patch Pipeline & Vulnerability Scan Checklist Şablonu — Yazılım / Sunucu ve Güvenlik (v1.0)

Asset Amaç: Bu asset, sunucu ve sistem patch (yama) yönetimini ad-hoc/rastgele uygulamalardan çıkarıp Scan → Plan → Test → Deploy → Rollback adımlarından oluşan disiplinli bir pipeline'a dönüştürmek için hazırlanmıştır. Tespit edilen zafiyetlerin risk seviyelerine göre kapatılma hedeflerini (SLA) belirler ve staging testlerini canlıya geçiş öncesi zorunlu kılar. Olası uyumsuzluk durumlarında devreye girecek rollback adımlarını yazılı ve tatbik edilebilir bir runbook'a bağlayarak canlı ortam kesinti riskini en aza indirir.

Kim Kullanır?: Sistem Yöneticileri, DevOps / BT Ekipleri, Otel IT Yöneticileri ve B2B Platform Ekipleri.

Nasıl Kullanılır?

1. Altyapınız için zafiyet tarama periyodunu ve tespit edilen risk gruplarının kapatılma sürelerini (SLA) tanımlayın.
2. Güncellemeleri önce staging ortamında test edin, dökümante edilen duman (smoke) testlerinden geçirip planlı bakım penceresine alın.
3. Canlıya geçiş sonrası health-check adımlarını uygulayın; olumsuz bir durumda rollback prosedürünü çalıştırıp süreci raporlayın.

CHECKLIST & SPRINT PLAN — Patch Pipeline & Vulnerability Scan Şablonu

A) Ölçüm & Önceliklendirme Kontrol Listesi (Checklist)

- [ ] **Tarama Periyodu Tanımlı:** Zafiyet taramaları düzenli aralıklarla (haftalık/aylık) ve sistemlerdeki her büyük değişiklik sonrasında otomatik tetikleniyor.
- [ ] **Risk Sınıfları ve SLA'lar Yazılı:** Taranan bulgular (Kritik, Yüksek, Orta, Düşük) için net çözüm süreleri (Örn: Kritik için max 24-72 saat SLA) belirlendi.
- [ ] **Owner Ataması Net:** Her sunucu, servis ve uygulama katmanı için yamalama sorumlusu (Sistem/Uygulama Sahibi) atandı.
- [ ] **Staging / Test Akışı Var:** Tüm yama ve güncellemeler canlıya alınmadan önce izolasyonlu staging ortamında fonksiyonel testlerden geçiriliyor.
- [ ] **Bakım Penceresi Takvimi Var:** Kullanıcı trafiğinin en düşük olduğu zaman dilimlerinde (Örn: Gece 02:00-05:00) planlı bakım pencereleri dökümante edildi.
- [ ] **Rollback Yöntemi Seçili:** Olası bir sistem hatasında geri dönüş yöntemi (VM Snapshot, Paket Versiyon Düşürme, Container Rollback) önceden belirlendi.
- [ ] **Post-Deploy Health-Check Checklist'i Var:** Yama uygulandıktan hemen sonra servislerin, API'lerin ve veritabanı bağlantılarının çalıştığını doğrulayan kontrol seti hazır.
- [ ] **24–72 Saat Gözlem Planı Var:** Canlıya alınan patch sonrası sistem performansı, error log'ları ve kaynak kullanımı 1-3 gün boyunca yakın takibe alınıyor.
- [ ] **Rapor ve Kayıtlar KVKK Uyumlu Saklanıyor:** Zafiyet ve yama geçmişi kayıtları, KVKK teknik tedbirleri ve denetim standartlarına uygun biçimde erişim kısıtlı ortamda loglanıyor.

- [ ] **Büyük Upgrade'lerde CWV / Uptime İzleniyor:** İşletim sistemi veya ana framework yükseltmelerinde Core Web Vitals (CWV) ve servis erişilebilirlik (uptime) metrikleri izleniyor.

B) Problem → Kök Neden → Çözüm Tablosu

Problem	Kök Neden	Çözüm
Prod'da sürpriz kırılma	Yamaların doğrudan canlı ortamda uygulanması, Staging test katmanının bulunmaması.	Staging ortamında zorunlu test + otomatik smoke test adımı.
Süre bitmiyor / Yamalar gecikiyor	Hangi zafiyetin ne zaman kapatılacağına dair önceliklendirmenin yapılmaması.	Risk seviyelerine göre SLA belirleme + Sorumlu (Owner) atama.
Rollback panik ve uzayan kesinti	Yama patladığında geri dönüş adımlarını gösteren döküman olmaması.	Test edilmiş Rollback runbook'u + düzenli kriz tatbikatı.
Gürültü / Yanlış Alarmlar	Tarama araçlarının ürettiği yanlış pozitif (False-positive) bulguların elenmemesi.	Risk doğrulama adımının sürece eklenmesi + iteratif muafiyet listesi.

C) 14 Günlük Patch Pipeline & Vulnerability Scan Sprint Planı

Hafta 1: Envanter, SLA ve Staging Test Kurgusu

- **Gün 1 (Varlık Envanteri & Tier Sınıflandırma):** Altyapıdaki tüm sunucu, VM ve servislerin envanterinin çıkarılması; kritiklik seviyelerine (Tier 1/2/3) göre gruplanması.
- **Gün 2 (Tarama Periyodu & SLA Seti):** Otomatik tarama periyotlarının konfigüre edilmesi ve CVSS skorlarına göre çözüm SLA'larının dökümante edilmesi.
- **Gün 3 (Tarama → Ticket → Owner Akışı):** Zafiyet tarama aracının Jira/ITSM sistemine entegre edilerek ilgili ekiplere otomatik görev atanması.
- **Gün 4 (Staging Patch Prosedürü & Smoke Test):** Staging ortamı güncelleme senaryolarının ve otomatik/manuel duman testlerinin hazırlanması.
- **Gün 5 (Bakım Penceresi & İletişim Planı):** Canlı ortam yama pencerelerinin takvime işlenmesi, iç ve dış paydaş bilgilendirme şablonlarının oluşturulması.
- **Gün 6 (Rollback Yöntemi ve Runbook):** Sistem bileşenleri bazında geri alma (snapshot restore, package rollback) adımlarının runbook haline getirilmesi.

- **Gün 7 (İlk Staging Patch Uygulaması):** Hazırlanan hattın staging sunucuları üzerinde ilk defa uçtan uca çalıştırılması.

Hafta 2: Prod Deploy, Health-Check ve Raporlama

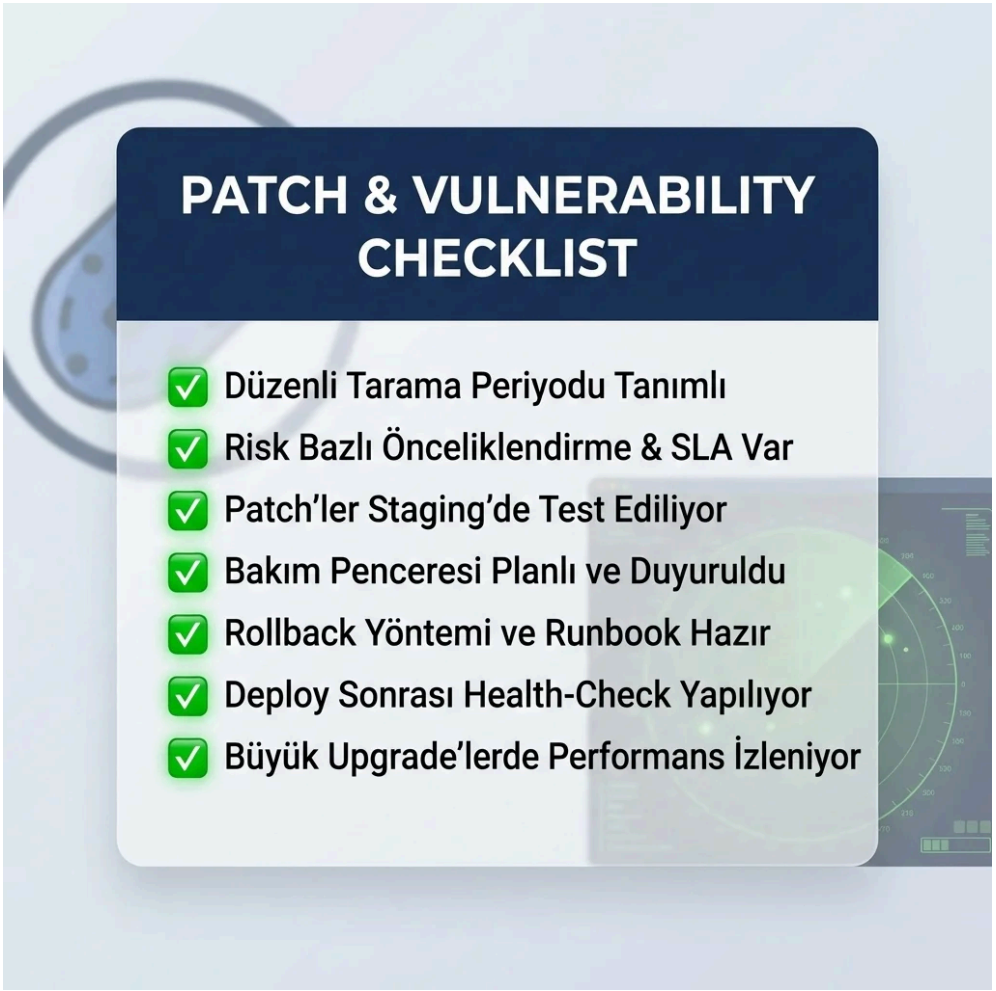
- **Gün 8 (Staging Doğrulama & Performans Kontrolü):** Staging ortamındaki yamalı sistemlerin performans, log ve işlevsellik testlerinin tamamlanması.
- **Gün 9 (Prod Deploy - Planlı Pencere):** Belirlenen bakım penceresinde canlı ortam sunucularına onaylı yamaların sırayla uygulanması.
- **Gün 10 (Post-Deploy Health-Check & İzleme):** Güncelleme sonrasında servis kontrol listesinin çalıştırılması ve 24 saatlik ilk gözlem sürecinin başlatılması.
- **Gün 11 (Kontrollü Rollback Tatbikatı):** Staging ortamında kasıtlı hata oluşturularak rollback runbook'unun çalışma hızının ve doğruluğunun test edilmesi.
- **Gün 12 (Rapor & Kapanış Metrikleri):** Kapatılan zafiyetlerin, ortalama kapatma sürelerinin (MTTR) ve başarı oranının raporlanması.
- **Gün 13 (Politika Güncelleme):** Süreçte yaşanan aksaklıklardan elde edilen öğrenimler doğrultusunda yama politikasının revize edilmesi.
- **Gün 14 (Sonraki Döngü Planı):** Bir sonraki ayın/dönemin zafiyet tarama ve yama takviminin onaylanarak otomasyona bağlanması.

D) Öncesi / Sonrası Durum KPI Tablosu

KPI Metriği	**Yöntem Öncesi (Mevcut Durum)**	**Yöntem Sonrası (Standart)**	**Hedef / Trend**
Kritik Bulgu Kapanma Süresi	45+ Gün (Plansız)	< 72 Saat (SLA Uyumlu)	**Hedef $\downarrow$** (Hızlı yama)
Rollback Sayısı / Başarısızlık	Yüksek / Belirsiz	$< \%2$ (Staging Filtreli)	**Hedef $\downarrow$** (Min. hata)
Planlı Bakım Penceresi Oranı	$\%20$ (Gündüz/Mesai içi)	$\%100$ (Gece/Planlı)	**Hedef $\uparrow$** (Tam kontrol)
Prod Kırılma Oranı	$\%15$ (Beklenmedik kesinti)	$\%0$ (Kesintisiz geçiş)	**Hedef $\downarrow$** (Sıfır sürpriz)

Deliverables (Teslim Edilecek Çıktılar)

- **Kurumsal Patch Politikası & Risk SLA Dokümanı:** Zafiyet derecelerine göre müdahale sürelerini ve kuralları içeren politika belgesi.
- **Zafiyet Tarama Planı & Otomatik Ticket Akış Şeması:** Taramadan görev atamaya kadar olan iş akış mimarisi.
- **Staging Test & Smoke Test Kontrol Listesi:** Canlı öncesi doğrulamada kullanılacak test adımları.
- **Acil Durum Rollback Runbook'u:** Olası aksaklıklarda sistemleri güvenli duruma döndürme kılavuzu.
- **Post-Deploy Health-Check & Denetim Rapor Şablonu:** Yama sonrası sistem sağlığını ve denetim kayıtlarını belgeleyen şablon.



[Checklist Card]

Sistem yöneticileri, DevOps ekipleri ve siber güvenlik uzmanları için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Patch Pipeline Kontrol Kartı. Koyu karbon gri ve koyu lacivert/yeşil tonlarındaki teknolojik zemin üzerinde; zafiyet tarama radar ikonu, CI/CD yama boru hattı (pipeline) akış şeması, staging doğrulama damgası ve geri sarma (rollback) dişli sembolleri yer alıyor. Kartın üzerinde; "Risk Bazlı SLA & Otomatik Ticket Akışı", "Staging Testi & Mandatory Smoke Tests", "Planlı Bakım Penceresi & Prod Deploy" ve "Rollback Runbook & Health-Check Verification" kontrol maddeleri, yanlarında

parlak yeşil onay işaretleriyle scannable ve kurumsal bir checklist formatında sergileniyor.