# Sunucu Hardening Baseline & Compliance Scan Planlama Şablonu — Yazılım / Sunucu ve Güvenlik (v1.0)

**Asset Amaç:** Bu şablon; CIS Benchmark (Center for Internet Security) veya benzeri uluslararası standartlardan kurumunuza özel bir sunucu sertleştirme (*hardening*) baseline'ı çıkarıp, agent veya script tabanlı uyumluluk taramaları (*compliance scan*) ile bu kuralları sürekli doğrulamak amacıyla hazırlanmıştır. DMZ/Web, API/Portal, Veritabanı ve Yönetim sunucuları gibi farklı rollerdeki sunucular için özelleştirilmiş güvenlik profilleri tanımlamanızı sağlar. Güncelleme veya yama (*patch*) uygulamaları sonrasında oluşabilecek konfigürasyon kaymalarını (*configuration drift*) erken tescil edip hızlıca aksiyona dönüştüren biletleme ve iyileştirme akışını standardize eder.

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

## Nasıl Kullanılır?

1. İşletim sistemi (OS) ve web sunucu/runtime envanterinizi çıkarıp referans alacağınız CIS Benchmark seviyesini seçin.
2. Sunucu rollerine göre (DMZ-Web, API/Portal vb.) profil bazlı sertleştirme kurallarını ve Pass/Fail ölçüm kriterlerini belirleyin.
3. Otomatik taranma periyodunu, tetikleyici olayları (patch/release sonrası) ve Rapor → Ticket → Fix iyileştirme döngüsünü tanımlayın.

## TEMPLATE — Sunucu Hardening Baseline & Compliance Scan Planı

### 1) Referans Benchmark Seçimi

- **İşletim Sistemi (OS):** Ubuntu Server 22.04 LTS / RHEL 9 / Windows Server 2022
- **Web Server / Runtime:** Nginx 1.24+ / Apache 2.4+ / Node.js LTS / Docker Engine
- **Referans Benchmark Standardı:** CIS Benchmark (Level 1 - Server & Level 2 - High Security) / NIST SP 800-123
- **Baseline Doküman Versiyonu:** v1.0 (Kurumsal Güvenlik Politikası Uyumlu)

### 2) Sunucu Profil Tanımları

| Profil | Kapsam | Örnek Sunucular | Özel Güvenlik Notu |
|---|---|---|---|
| **DMZ-Web** | Dış internete açık Reverse Proxy, WAF ve Web Ön Yüz sunucuları | web-proxy-01, lb-nginx-prod | Sıkılaştırılmış SSH, strict TLS 1.3, unprivileged process |

| | | | |
|---|---|---|---|
| **API / Portal** | İş mantığını ve B2B/Otel API servislerini barındıran iç/dış sunucular | api-gateway-01, pms-sync-02 | Kısıtlı outbound IP kuralı, AppArmor/SELinux zorunlu |
| **DB / Data (Isolated)** | Müşteri, finans ve otel rezervasyon verilerini tutan veritabanları | db-pg-master, redis-cache-prod | İnternet erişimi sıfır, şifrelenmiş disk (LUKS), kısıtlı sudo |
| **Mgmt / Infra** | CI/CD, Bastion Host, İzleme ve Log sunucuları | bastion-ssh, grafana-prod | Yalnızca VPN/MFA üzerinden erişim, kısıtlı root execution |

**3) Baseline Kontrol Seti (Pass / Fail Matrisi)**

| Kontrol Alanı | Kural & Sertleştirme Standardı | Ölçüm / Doğrulama Yöntemi | Durum | İstisna (Varsa) |
|---|---|---|---|---|
| **Erişim (Auth & SSH)** | Root login kapalı (PermitRootLogin no), Parolasız SSH Key / Certificate zorunlu, Default port değiştirildi. | sshd -T \| grep permitrootlogin | **Pass** | Yok |
| **Port / Servis** | Kullanılmayan tüm portlar kapalı, varsayılan servisler (telnet, ftp, rsh) kaldırıldı, UFW/Firewalld aktif. | netstat -tuln, systemctl status | **Pass** | Yok |

| | | | | |
|---|---|---|---|---|
| **Log / Audit** | auditd aktif, kritik sistem dosyaları (/etc/passwd, /etc/shadow) izlemede, Rsyslog/Fluentd uzak SIEM'e bağlı. | auditctl -l, systemctl status auditd | **Pass** | Yok |
| **Patch / Drift Kontrol** | Kernel ve paket güncellemeleri yapılmış, yetkisiz dosya izin değişiklikleri (chmod 777) engellenmiş. | unattended-upgrades --dry-run, find / -perm 777 | **Pass** | Eski legacy paket için geçici izin |

**4) Compliance Scan (Uyumluluk Taraması) Tasarımı**

- **Tarama Yöntemi:** Agent-based (Wazuh Agent / Nessus Agent) & Script-based (OpenSCAP / CIS-CAT / Ansible InSpec)
- **Otomatik Tarama Periyodu:** Haftalık Otomatik Taramalar (Her Pazar Gece 03:00)
- **Tetikleyici Olaylar (Triggers):**
  - OS Yama / Kernel Güncellemesi (Patch) Sonrası
  - Yeni Sürüm / Uygulama Yayınlama (Release) Sonrası
  - Sistem Konfigürasyon Değişikliği (Ansible Playbook execution) Sonrası
- **Rapor Formatı:** HTML Dashboard / JSON / PDF Executive Summary
- **Sorumlu Owner & İyileştirme SLA'sı:**
  - **Kritik Fail (Score $< \%70$):** SysAdmin Team — SLA: **24 Saat**
  - **Yüksek/Orta Fail (Score $\%70-\%90$):** DevOps Team — SLA: **7 Gün**

**5) İstisna & Sapma Yönetimi (Exception Management)**

- **Gerekçe Zorunluluğu: Evet (Zorunlu)** — Basit teknik gerekçeler kabul edilmez; iş etkisi ve telafi edici kontrol (*compensating control*) belirtilmesi şarttır.
- **Geçerlilik Süresi / Otomatik Kapanış:** Maksimum **90 Gün** (Süre sonunda istisna otomatik düşer ve tekrar tarama başarısız gözükür).
- **Onay Akışı:** Bilgi Güvenliği Yöneticisi (CISO / Security Lead) + BT Direktörü Onayı.

**6) Denetim ve Kontrol Listesi (Checklist)**

- [ ] **Baseline Profilleri Ayrıldı:** Web, API, DB ve Yönetim sunucuları için farklı sertleştirme seviyeleri tanımlandı.
- [ ] **Pass / Fail Ölçüm Kriterleri Tanımlı:** Otomatik tarama araçlarının doğrulayabileceği somut komutlar/parametreler belirlendi.
- [ ] **Scan Periyodu ve Tetikleyiciler Net:** Haftalık rutin taramaların yanı sıra patch ve release sonrası otomatik taramalar kurgulandı.
- [ ] **Rapor $\rightarrow$ Ticket $\rightarrow$ Fix Akışı Var:** Taramada ortaya çıkan konfigürasyon kaymaları (drift) otomatik Jira/ITSM bileti olarak sorumlu ekibe atanıyor.

- [ ] **Revizyon Takvimi Yılda Bir (365 Gün) Güncelleniyor:** CIS Benchmark güncellemeleri ve yeni tehdit modellerine göre yılda bir kez baseline seti gözden geçiriliyor.

## Deliverables (Teslim Edilecek Çıktılar)

- **Sunucu Hardening Baseline Politikası & Profil Dokümanı (v1.0):** OS ve Web sunucu sertleştirme standartlarını belirten teknik rehber.
- **OpenSCAP / Ansible Automation Hardening Playbook Seti:** Sunucuları otomatik olarak CIS standartlarına getiren ve tarayan kod kütüphanesi (*Infrastructure as Code*).
- **Compliance Scan & Configuration Drift Rapor Şablonu:** Taramalar sonucu üretilen Pass/Fail durumunu ve drift analizini gösteren rapor paneli.
- **İstisna / Sapma (Exception) Onay Formu & Takip Kaydı:** Sistem zorunlulukları nedeniyle uygulanamayan kuralların kayıt ve denetim formu.


**[Deliverables / Proof Card]**

*Sistem yöneticileri, siber güvenlik denetçileri ve DevOps liderleri için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Server Hardening Deliverables Kartı. Koyu karbon gri ve amber/yeşil kalkan tonlarındaki teknolojik zemin üzerinde; CIS Benchmark uyumluluk rozeti, sunucu sertleştirme kontrol listesi, OpenSCAP otomatik compliance tarama göstergesi*

*ve kilitli sunucu kule simgeleri yer alıyor. Kartın üzerinde; "Role-Based CIS Hardening Baselines (DMZ/API/DB)", "Automated OpenSCAP & Agent Compliance Scans", "Configuration Drift Detection & Auto-Ticketing" ve "Formal Exception Management & 365-Day Review" teslimat kalemi başlıkları, yanlarında parlak yeşil onay işaretleriyle scannable ve kurumsal bir proof-card formatında sergileniyor.*