“Terraform/Ansible Güvenlik Konfigürasyonu” Planlama Şablonu — Yazılım / Sunucu ve Güvenlik (v1.0)

Asset Amaç: Bu şablon; güvenlik duvarı (*security group/firewall*), kullanıcı yetkilendirmeleri, sistem paket baseline'ları ve hardening adımlarını Terraform ve Ansible kullanarak *Security-as-Code* (Kod Olarak Güvenlik) yaklaşımında planlamak için hazırlanmıştır. Repository → Plan → Apply CI/CD süreçlerinde hangi kontrol noktalarının bulunması gerektiğini netleştirir. Altyapı sapmalarını (*configuration drift*) en aza indirmeyi ve *"Bu portu kim açtı?"* belirsizliğini Pull Request (PR) geçmişiyle tamamen izlenebilir kılmayı hedefler.

Kim Kullanır?: DevOps/BT Ekipleri, Ajans Teknik Liderleri, Otel IT Sorumluları ve B2B Platform Ekipleri.

Nasıl Kullanılır?

1. Mevcut altyapıdaki güvenlik ayarlarının envanterini çıkarın ve kod olarak yönetilecek (*Infrastructure as Code*) bileşenleri işaretleyin.
2. Terraform modülleri (altyapı) ve Ansible rolleri (konfigürasyon) için planı doldurun; Staging ve Production ortam farklılıklarını tanımlayın.
3. PR review zorunluluklarını, onay mekanizmalarını ve *drift* (yapısal sapma) doğrulama periyotlarını belirleyerek pipeline yönetişimini kilitleyin.

TEMPLATE — Terraform / Ansible Güvenlik Konfigürasyonu Planlama Şablonu

1) Ortam ve Kapsam Tanımlama Formu

Parametre	Detay / Giriş Alanı
Proje Tipi	[ ] Otel Operasyon (PMS/Web) | [ ] B2B SaaS Platform | [ ] Ajans Altyapısı
Hedef Ortamlar	[ ] Development | [ ] Staging | [ ] Production
Sunucu Rol Seti	[ ] Web Server (Nginx) | [ ] App/API Server (Node/Python) | [ ] DB Server (PostgreSQL/Redis)

Kritik İş Yükleri	_____ ___ *(Örn: Ödeme Geçidi, PMS Entegrasyon API, Kullanıcı Rıza Logları)*

2) Güvenlik Ayar Envanteri (Koda Taşınacaklar Matrisi)

Ayar Kategorisi	Şu An Nasıl Yönetiliyor?	Hedef (Terraform / Ansible)	Öncelik (1–5)
Security Group / Firewall	Manuel AWS Console / UFW komutları	Terraform aws_security_group modülü	**5 (Kritik)**
Kullanıcı / Rol / Sudo	Sunucularda manuel useradd / visudo	Ansible user ve sudoers rolleri	**4 (Yüksek)**
Paket Baseline	Manuel apt upgrade / Rastgele güncellemeler	Ansible idempotent paket kütüphanesi	**3 (Orta)**
SSH Hardening	Varsayılan SSH (Port 22, Password Auth Açık)	Ansible SSH Hardening Role (Port/Key-only)	**5 (Kritik)**
Log / Agent Kurulumu	Manuel log-rotate ve agent indirme	Ansible CloudWatch / Syslog agent rolu	**4 (Yüksek)**

3) Terraform Planı (Kaynak ve Mimari Yönetimi)

- **Modül Listesi:**
  - modules/vpc_network: VPC, subnet ve route table yapılandırması.
  - modules/security_groups: Rol bazlı (Web, App, DB) izole güvenlik duvarı kuralları.
  - modules/iam_roles: En az yetki prensipli (*Principle of Least Privilege*) IAM rol ve politikaları.
- **Ortam Bazlı Değişkenler (Staging vs. Prod):**

    - *Staging:* Sadece ofis IP bloklarına açık SSH (/32), dinamik test veritabanı portları.
    - *Prod:* SSH trafiği tamamen kapalı (yalnızca Bastion/SSM over Private Subnet), katı IP white-listing.
- **Plan-Review Kontrol Listesi:**
    - [ ] terraform plan çıktısında yıkıcı (*destructive*) bir değişiklik var mı?
    - [ ] Açılan portlar mimari standartlara uygun mu (Örn: DB portu dışarıya kapalı mı)?
- **State Saklama & Erişim Yaklaşımı:**
    - AWS S3 Remote Backend + DynamoDB State Locking (AES-256 şifreli, halka kapalı kova).

4) Ansible Planı (Konfigürasyon ve Sunucu Hardening)

- **Role Listesi (Idempotent Yapı):**
    - roles/common_baseline: Temel sistem paketlerinin ve güvenlik güncellemelerinin yüklenmesi.
    - roles/ssh_hardening: Root girişinin kapatılması, parola ile girişin engellenmesi, özel port tanımı.
    - roles/firewall_ufw: Sunucu içi *iptables/ufw* kurallarının sıfırlanıp sadece gerekli portların izinlendirilmesi.
- **Paket / Servis Baseline:**
    - Gereksiz servislerin (telnet, ftp, rsh) durdurulması ve sistemden kaldırılması.
    - Otomatik güvenlik güncellemelerinin (unattended-upgrades) aktif edilmesi.
- **Kullanıcı & Yetki Politikası:**
    - Bireysel SSH anahtarlarının (*Public Key*) sunuculara otomatik dağıtımı.
    - Paylaşımlı root kullanımının yasaklanması; tüm adımların sudo loglama ile kişiselleştirilmesi.
- **SSH & Host İçi Güvenlik Ayarları:**
    - PermitRootLogin no, PasswordAuthentication no, MaxAuthTries 3, X11Forwarding no.

5) Pipeline ve Governance (CI/CD Yönetişimi)

- **Repository Yapısı:** Monorepo yapısında /terraform ve /ansible dizinlerinin ayrılması; hassas verilerin (vars/vault.yml) Ansible Vault ile şifrelenmesi.
- **PR Onay Kuralı (Reviewer Policy):** main branch'e yapılacak her PR için en az **2 Senior DevOps / Security** mühendisinin onay zorunluluğu.
- **Plan Çıktısı Saklama:** CI/CD runner tarafından oluşturulan tfplan dosyalarının artefact olarak **30 gün** güvenli saklanması.
- **Apply Yetkisi (Kim / Nerede):** Geliştirici makinelerinden manuel apply yasaktır. Yalnızca CI/CD botu (OIDC token onaylı) üzerinden tetiklenir.
- **Drift Kontrol Periyodu:** Her gece otomatik terraform plan çalıştırılarak altyapıda manuel değişiklik yapılıp yapılmadığının tespiti ve Slack/Teams alarmı.

6) Denetim ve Kontrol Listesi (Checklist)

- [ ] **Security Group Kuralları Modülleştirildi:** Tüm güvenlik duvarı kuralları kod haline getirildi, arayüzden manuel müdahale engellendi.
- [ ] **Ansible Hardening Rolleri Idempotent:** Oyun kitapları (*playbooks*) defalarca çalıştırılsa dahi sistem durumunu bozmayacak şekilde test edildi.

- [ ] **State Güvenliği Sağlandı:** Terraform .tfstate dosyaları uzaktaki şifreli backend'e alındı ve erişim yetkileri kısıtlandı.
- [ ] **PR + Review Zorunluluğu Aktif:** Kod incelemesi olmadan hiçbir güvenlik konfigürasyonunun canlıya alınamayacağı pipeline kuralı koyuldu.
- [ ] **Drift Raporu ve Geri Alma Süreci Var:** Manuel müdahaleler gece taramalarıyla yakalanıyor ve sürüm geçmişindeki kararlı sürüme (*Git Rollback*) dönülebiliyor.

Deliverables (Teslim Edilecek Çıktılar)

- **Terraform / Ansible Güvenlik Konfigürasyon Planlama Şablonu (v1.0):** Ortam, değişken ve modül eşleşmelerini içeren mimari döküman.
- **IaC Pipeline Governance & Drift Yönetim Prosedürü:** CI/CD onay mekanizmalarını ve nightly-drift tarama standartlarını tanımlayan kılavuz.
- **Hardening & Security Baseline Checklist:** Sunucu ve ağ seviyesinde uygulanacak güvenlik sertleştirme adımlarının kontrol listesi.

[Deliverables / Proof Card]

DevOps mühendisleri, sistem mimarları ve güvenlik liderleri için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Infrastructure as Code (IaC) güvenlik teslimat kartı. Koyu karbon gri ve siber yeşil tonlarındaki teknolojik zemin üzerinde, Terraform kilit simgesi, Ansible playbook ikonu ve kod tarama büyüteci görselleri yer alıyor. Kartın üzerinde; "Security-as-Code Envanter Matrisi", "Idempotent Ansible Hardening Rolleri", "Remote Encrypted State & Lock" ve "Nightly Drift Detection Pipeline" teslimat kalemi başlıkları, yanlarında parlak onay işaretleriyle scannable ve kurumsal bir proof-card formatında sergileniyor.