CI/CD İçin DevSecOps Güvenlik Gate Planlama Şablonu — Yazılım / Sunucu ve Güvenlik (v1.0)

Asset Amaç: Bu şablon; CI/CD süreçleri içerisine güvenlik kapılarını (*security gates*) doğru aşamalara yerleştirmek ve engelleme eşiklerini kademeli olarak sertleştirmek için hazırlanmıştır. Secret scanning, SAST, SCA ve IaC policy check çıktılarının otomatik olarak iş takip sistemlerine (*jira/backlog*) aktarılmasını ve kritik zafiyet tespitinde canlıya çıkışın (*release*) engellenmesini standardize eder. Temel amaç, prodeksiyon ortamına zafiyet taşıma oranını ve acil yamalama (*hotfix*) ihtiyacını en aza indirmektir.

Kim Kullanır?: DevOps / Platform Lead'leri, Güvenlik Liderleri, Backend Lead'leri ve Release Sorumluları.

Nasıl Kullanılır?

1. CI/CD boru hattı adımlarınızı (*commit →build →test →deploy*) haritalandırıp her güvenlik kapısının (*gate*) yerleşeceğini noktayı belirleyin.
2. Güvenlik testlerinin eşik kademelerini (*uyarı/warning →engelleme/block*) ve bulgu SLA sürelerini tanımlayın.
3. Otomatikleştirilmiş "Bulgu → Backlog →Düzeltme →Re-test" doğrulama döngüsünü ekleyerek planlamayı tamamlayın.

TEMPLATE — CI/CD DevSecOps Güvenlik Gate Planlama Şablonu

1) Pipeline Haritası Tablosu

Aşama	Araçlar	Çıktı	Not
Commit / MR	_____	_____	_____
Build	_____	_____	_____
Test	_____	_____	_____
Deploy	_____	_____	_____

2) Gate Yerleşimi Tablosu

Gate	Çalıştığı Aşama	Fail Kriteri	Aksiyon
Secret Scan	_____	_____	**Merge Block**
SCA	_____	_____	**Ticket + SLA**
SAST	_____	_____	**Warn →Block**
Policy Check	_____	_____	**Deploy Block**

3) Eşik Kademesi (Threshold Staging)

- **Faz-1 (Görünürlük & Warning Modu):** _____ *(Tüm taramalar aktif, build durdurulmaz, zafiyetler backlog'a aktarılır)*
- **Faz-2 (Kritik Blok Modu):** _____ *(Secret sızıntıları ve Kritik [CVSS 9.0+] zafiyetlerde derleme/merge otomatik engellenir)*
- **Faz-3 (Orta Sevesi Sertleşme & Tam Otomasyon):** _____ *(Yüksek/Orta seviye bulgularda SLA aşımında deploy durdurulur, IaC policy check kısıtları devreye girer)*

4) Bulgu Yönetimi (Backlog & SLA)

- **Owner Atama Kuralı:** _____ *(Kodun yazarı / İlgili squad lead)*
- **Kritik Bulgu Hedef SLA:** _____ *(Örn: 24-48 Saat)*
- **Yüksek / Önemli Bulgu Hedef SLA:** _____ *(Örn: 7 Gün)*
- **Re-test Zorunluluğu:** (E/H) [ ] *(Kod PR'a tekrar push edildiğinde otomatik re-scan koşar)*
- **Exception Prosedürü (Geçici Risk Acceptance):**
  - **Süre Limit:** _____ *(Max 14/30 gün)*
  - **Gerekçe:** _____
  - **Onay Yöneticisi & Kapanış Tarihi:** _____ / ___/___/2026

5) Kontrol Listesi (Checklist)

- [ ] **Secret Scanning:** Tüm commit ve PR'larda sızıntı taraması aktif, gizli bilgi tespitinde derleme *istisnasız engelleniyor (Merge Block)*.
- [ ] **SCA Entegrasyonu:** Yazılım bağımlılıkları *lockfile* (package-lock.json, Pipfile.lock vb.) üzerinden taranarak bilinen CVE'ler backlog'a biletleniyor.
- [ ] **IaC & Deployment Policy Check:** Kubernetes manifestleri ve Terraform dosyaları canlıya çıkış öncesi *Opa/Kyverno/Checkov* ile denetleniyor *(Deploy Block)*.
- [ ] **Backlog & Re-test Döngüsü:** Kapatılan zafiyetlerin doğrulanması için otomatik re-test pipeline tetikleyicisi kurgulandı.
- [ ] **180 Günlük Kalibrasyon Takvimi:** Güvenlik kapılarının yanlış pozitif (*false positive*) oranları ve SLA süreleri 6 ayda bir gözden geçiriliyor.

Deliverables (Teslim Edilecek Çıktılar)

- **DevSecOps Pipeline Güvenlik Gate Şablonu (v1.0):** Taramaların çalışacağı aşamaları ve kural matrislerini içeren ana doküman.
- **Kademeli Sertleştirme (Warn-to-Block) Matrisi:** Geliştirici adaptasyonunu bozmadan kapıları sertleştirme stratejisi rehberi.
- **Automated Ticket & Re-test Akış Şeması:** Taranan zafiyetlerin iş takip sistemlerine aktarılması ve fix doğrulaması iş akışı.
- **Geçici İzin / Exception Yönetim Protokolü:** Süreli risk kabul ve onay mekanizmaları kural seti.

[Proof Card]

DevOps liderleri, güvenlik uzmanları ve release yöneticileri için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir DevSecOps Proof Kartı. Koyu karbon gri zemin üzerinde; CI/CD pipeline hattı boyunca konumlandırılmış parlak mavi, yeşil ve kırmızı güvenlik kapıları (Secret Scanning, SAST, SCA, Policy Check). Kartın üzerinde; "Automated Commit-to-Deploy Security Gates", "Staged Threshold Rules: Warn to Block Transition", "Jira/Backlog Integrated Ticket & Re-Test Loops", ve "Time-bound Exception & Risk Acceptance Protocol" teslimat kalemi başlıkları, yanlarında yeşil onay rozetleriyle scannable ve kurumsal bir proof-card formatında sergileniyor.