Pentest + CI/CD Entegre Sürekli Güvenlik Testi Planlama Şablonu — Yazılım / Sunucu ve Güvenlik (v1.0)

Asset Amaç: Bu şablon; otel ve B2B projelerinde penetrasyon testini periyodik olarak planlarken, DAST, SAST ve SCA denetimlerini CI/CD boru hatlarına entegre eden "sürekli güvenlik testi" modelini kurmak için hazırlanmıştır. Tarafınıza iletilen güvenlik bulgularının risk önceliğine göre sprint bazlı çözülmesini ve her kritik zafiyetin re-test ile doğrulanmasını standardize eder.

Kim Kullanır?: Güvenlik Liderleri, DevOps / Backend Lead'leri, QA / Release Sorumluları ve Ajans Teknik Yöneticileri.

Nasıl Kullanılır?

1. Projenizdeki test yüzeylerini (Web, API, Mobil vb.) ve kritik iş akışlarını (*rezervasyon, ödeme, üye portalı*) listeleyin.
2. DAST, SAST ve SCA araçlarını CI/CD pipeline kapılarına (*gate*) bağlayarak çalıştırma frekanslarını belirleyin.
3. Bulgu çözüm SLA'larını, remediation sprint süreçlerini ve re-test doğrulama akışını tanımlayarak planlamayı tamamlayın.

TEMPLATE — Sürekli Güvenlik Testi & Pentest Planlama Şablonu

1) Kapsam Envanteri Tablosu

Yüzey	Kapsam	Kritiklik (1–5)	Not
Web	_____	[ ]	_____
API	_____	[ ]	_____
Mobil	_____	[ ]	_____

Altyapı	_____	[ ]	_____
Entegrasyon (PMS / CRM / Ödeme)	_____	[ ]	_____

2) Test Türleri ve Frekans Tablosu

Test	Araç / Yaklaşım	Nerede Çalışır?	Frekans	Gate?
SAST	_____	**PR / CI**	_____	**E / H**
SCA	_____	**PR / CI**	_____	**E / H**
DAST	_____	**Staging**	_____	**E / H**
Pentest	**Black / Gray / White Box**	**Prod Benzeri**	_____	—
Re-test	_____	**Staging / Prod**	**Her Kritik Bulguda**	**Evet**

3) Bulgu Yönetimi (SLA)

- **Kritik Bulgu Hedef Kapanış Süresi:** _____ (Örn: 24-48 Saat)
- **Önemli Bulgu Hedef Kapanış Süresi:** _____ (Örn: 7 Gün)

- **Düşük Bulgu Hedef Kapanış Süresi:** _____ (Örn: 30 Gün)
- **Owner Atama Kuralı:**
  _____
- **Re-test Zorunluluğu:** (E/H) [ ]

4) CI/CD Policy Gate

- **SAST Fail Kriteri:** _____
- **SCA Fail Kriteri (Kritik CVE):**
  _____
- **DAST Fail Kriteri (OWASP Top 10):**
  _____
- **Exception Prosedürü (Süreli Risk Kabul):**
  _____

5) Takvim

- **Yıllık Pentest Ayı:** _____
- **Büyük Release Sonrası Ek Test:** _____
- **Sezon / Peak Öncesi Ek Test (Otel):** _____
- **Export / Rapor Yoğunluğu Öncesi Ek Test (B2B):** _____

Şablon Kılavuzu & Uygulama

Nasıl Doldurulur? (5 Altın Kural)

1. **Önceliklendirin:** "Her şeyi her an test edelim" yaklaşımı yerine ödeme, üyelik ve rezervasyon gibi kritik akışları birinci öncelik yapın.
2. **Gateleri Kademeli Sertleştirin:** CI/CD üzerindeki güvenlik engellerini ilk günlerde "uyarı/warning", süreç oturdukça "derlemeyi durdur/block" şeklinde kademeli olarak devreye alın.
3. **Kanıt ile Kapatın:** Her kritik ve yüksek seviyeli bulgu için re-test şartı arayın; ilgili zafiyetin kapatılması ancak teknik kanıt gösterilerek onaylanmalıdır.
4. **Exception'ları Kurala Bağlayın:** İstisnai durumlarda (*risk acceptance*) geçici onay verilmesi gerekiyorsa bunun geçerlilik süresi, onaylayan yöneticisi ve gerekçesi mutlaka sisteme işlenmelidir.
5. **Bakım Döngüsüne Entegre Edin:** Güvenlik test takvimini, yazılım ekibinin rutin bakım-destek sprint'leriyle senkronize edin.

Uygulama Örneği (Kısa Senaryo)

- **SCA (Bağımlılık Taraması):** Her Pull Request (PR) aşamasında otomatik çalışır; bağımlılıklarda kritik bir CVE tespit edilirse *merge* işlemini otomatik engeller.
- **DAST (Dinamik Tarama):** Staging ortamında haftalık periyotta otomatik koşar; özellikle /login, /booking ve ödeme alma endpoint'leri taranır.
- **Pentest (Sızma Testi):** Yılda 1 kez bağımsız 3. taraf ekiplerce gerçekleştirilir; ilave olarak yaz sezonu öncesinde rezervasyon akışına özel sızma testi uygulanır.

Kontrol Listesi

- [ ] Kapsam ve kritik iş akışları detaylıca dökümante edildi.
- [ ] SAST ve SCA taramaları CI/CD boru hatlarında PR kapılarına (*PR gate*) bağlandı.
- [ ] DAST taramaları Staging ortamında düzenli takvime oturtuldu.

- [ ] Bulgu SLA süreleri, sorumlu (*owner*) atama yöntemi ve re-test zorunluluğu tanımlandı.
- [ ] Güvenlik test takvimi release ve bakım-destek sprint döngüleriyle uyumlu hale getirildi.

Deliverables (Teslim Edilecek Çıktılar)

- **Pentest & CI/CD Entegre Güvenlik Planlama Şablonu (v1.0):** Test türlerini, kapsamı ve takvimi yöneten çalışma dokümanı.
- **CI/CD Security Gate Kural Seti & Exception Formu:** PR/Build aşamalarında otomatik engelleme kriterleri ve süreli risk kabul protokolü.
- **Bulgu Yönetimi & SLA Takip Rehberi:** Zafiyet seviyelerine göre müdahale süreleri ve re-test doğrulama standartları.

[Proof Card]

Güvenlik liderleri, DevOps yöneticileri ve release sorumluları için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Pentest & Continuous Testing Proof Kartı. Koyu karbon gri ve canlı yeşil/mavi/kırmızı tonlarındaki teknolojik zemin üzerinde; CI/CD pipeline üzerindeki güvenlik kapıları (SAST/SCA/DAST), periyodik pentest takvimi, re-test doğrulama döngüleri ve SLA matrisi yer alıyor. Kartın üzerinde; "Continuous CI/CD Automated Security Gates", "Scheduled Periodic Pentest & Re-Test Loops", "Remediation SLA & Owner Mapping", ve "Time-bound Exception Management" teslimat kalemi başlıkları, yanlarında onay rozetleriyle scannable ve kurumsal bir proof-card formatında sergileniyor.