

Security Chaos Deneyleri & Senaryo Tasarımı Planlama Şablonu — Yazılım / Sunucu ve Güvenlik (v1.0)

Asset Amaç: Bu şablon; güvenlik kontrollerini ve olay müdahale (*incident*) süreçlerini küçük, kontrollü güvenlik chaos deneyleriyle proaktif olarak test etmek için hazırlanmıştır.

Deneylerin etki alanını (*blast radius*) kesin sınırlarla kısıtlamayı, tespit ve müdahale sürelerini (MTTD/MTTR) ölçülebilir kılmayı ve elde edilen öğrenimleri doğrudan backlog, güvenlik politikası ve runbook güncellemelerine dönüştürmeyi hedefler. KVKK/GDPR ve hizmet kesintisi (*uptime*) risklerini sınırlamak adına "kontrollü test ortamı" kuralını zorunlu kılar.

Kim Kullanır?: Güvenlik Liderleri, DevOps / SRE Mühendisleri, Platform Ekipleri ve Otel / B2B Operasyon Liderleri.

Nasıl Kullanılır?

- Deney senaryosunu seçin; test edilecek hipotezi ve başarı/başarısızlık kriterlerini netleştirin.
- Enjeksiyon planını (*kapsam, süre, otomatik geri alma / rollback*) ve gözlem metriklerini tanımlayın.
- Deney sonrasında elde edilen öğrenimleri (*Learn*) iş listelerine (*backlog*) aktarıp re-test ile doğrulanmasını sağlayın.

TEMPLATE — Security Chaos Deneyleri & Senaryo Tasarımı Planlama Şablonu

1) Deney Tanımı

- Deney Adı:** _____
- Amaç:** _____
- Hipotez (Beklenen Davranış):** _____
- Kapsam (İlgili Servis / Altyapı Katmanı):** _____
- Ortam Seçimi:** ☐ Staging / Lab | ☐ Prod-Benzeri Kontrollü Ortam
- Blast Radius Sınırı (Etki Alanı Limiti):** _____

2) Inject Planı Tablosu

Adım	Inject (Müdahale / Zafiyet Simülasyonu)	Süre	Rollback (Geri Alma Adımı)
1	_____	_____	_____

2			
3			

3) Observe (Ölçüm & İzleme)

- **MTTD Hedefi (Algılama / Tespitte Geçen Süre):** < _____ dakika
- **MTTR Hedefi (Çözüm / Müdahalede Geçen Süre):** < _____ dakika
- **Alarm Kanalı & Eskalasyon Akışı:**

- **Log & Metric Kaynakları (SIEM / APM):**

4) Learn (Öğrenim & Aksiyon Planı)

- **Deney Bulguları:** _____
- **Kök Neden Analizi (Kök Neden - Süreç / Araç Eksikliği):**

- **Backlog Aksiyonları (Jira / Task ID):**

- **Policy & Runbook Güncelleme Notları:**

- **Re-Test Planı Tarihi:** ____/____/2026

5) Risk ve Uyum Değerlendirmesi

- **KVKK / Veri Riski Değerlendirmesi:**
_____ (Anonim/Sentetik veri kullanımı zorunluluğu)
- **Uptime Riski & SLA Etkisi:**

- **Onay & Koordinasyon (Bakım / Destek / Ops):**
 - **Onay Veren:** _____
 - **Bilgilendirilen Ekipler:** _____
 - **Test Penceresi (Zaman Aralığı):** ____:____ - ____:____

6) Kontrol Listesi (Checklist)

- **[] Blast Radius Sınırlı:** Deneyin etki alanı tek bir pod, container veya isolated subnet ile kesin olarak kısıtlandı.
- **[] Rollback Adımı Yazılı & Hazır:** Deney kontrolden çıktığında veya süre dolduğunda otomatik devreye girecek iptal mekanizması test edildi.
- **[] KPI Ölçümü Net:** Algılama (MTTD) ve müdahale (MTTR) sürelerini ölçecek izleme ekranları active durumda.
- **[] Aksiyonlar Backlog'a Girdi:** Tespiti yapılan tüm eksik ve iyileştirmeler için ilgili geliştirme ekibine bilet açıldı.

- [] **Re-Test Planlandı:** Aksiyonlar tamamlandıktan sonra aynı senaryonun tekrar koşulacağı doğrulama tarihi takvime eklendi.
- [] **KVKK ve Bakım-Destek Koordinasyonu Yapıldı:** Müşteri verisi riski ekarte edildi; operasyon ve destek ekipleri test öncesinde bilgilendirildi.

Deliverables (Teslim Edilecek Çıktılar)

- **Security Chaos Deney Planlama Şablonu (v1.0):** Senaryo, hipotez ve inject adımlarını içeren standart çalışma dokümanı.
- **Blast Radius & Rollback Güvenlik Prosedürü:** Kontrol dışı durumlar için acil durdurma ve otomatik eski hale getirme protokolü.
- **Observe & KPI İzleme Dashboard Şablonu:** MTTD/MTTR metriklerinin real-time takip edildiği izleme paneli taslağı.
- **Learn-to-Backlog Döngüsü & Re-Test Takvimi:** Deney çıktılarının geliştirme ve güvenlik backlog'larına dönüştürülme rehberi.



[Proof Card]

Güvenlik mimarları, SRE liderleri ve platform mühendisleri için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Security Chaos

Engineering Proof Kartı. Koyu karbon gri zemin üzerinde; kırmızı ve turuncu kontrollü enjeksiyon simgeleri (fault injection), koruyucu yeşil blast-radius çemberi, MTDD/MTTR ölçüm sayaçları ve chaos test akış şeması. Kartın üzerinde; "Controlled Security Fault Injections & Hypotheses", "Strict Blast Radius Boundaries & Auto-Rollback Rules", "Measured Detection (MTDD) & Response (MTTR) Metrics", ve "Learn-to-Backlog Actions with Re-Test Verification" teslimat kalemi başlıkları, yanlarında yeşil onay ikonlarıyla scannable ve kurumsal bir proof-card formatında sergileniyor.