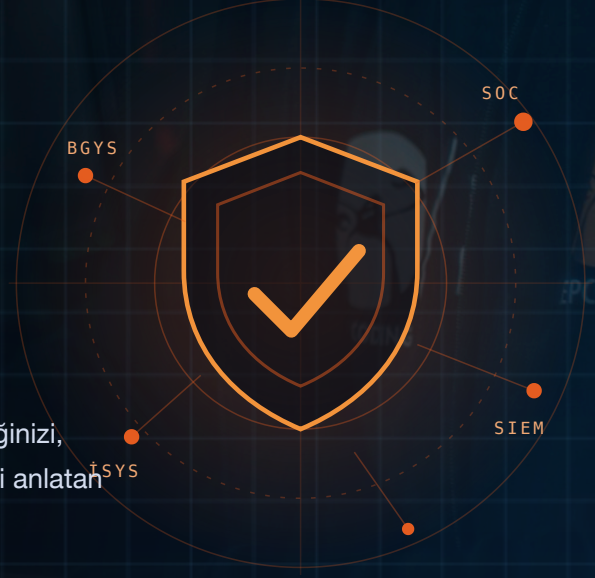


REHBER

Sızma Testine Hazırlık Rehberi

İlk sızma testinizi planlıyorsanız: kapsamı nasıl belirleyeceğinizi, neleri hazırlayacağınızı ve raporu nasıl değerlendireceğinizi anlatan pratik bir rehber hazırladık.



REHBER

YAKLAŞIK 7 DK OKUMA

SIZMA TESTİ

BU REHBERDE

1. Sızma testi neyi cevaplar?
2. Test türleri
3. Kapsam ve kuralları belirlemek
4. Test öncesi hazırlık listesi
5. Test süreci nasıl işler?
6. Raporu nasıl okumalı?

01 Sızma testi neyi cevaplar?

Zafiyet taraması bilinen zayıflıkların listesini çıkarır. Sızma testi ise yetkili bir uzmanın bir saldırgan gibi düşünerek açıkları birleştirmesi ve gerçekte nereye ulaşılabilirdiğini kanıtlamasıdır. Yani soru “hangi açıklarım var?” değil, “bir saldırgan neye ulaşabilir?” sorusudur.

02 Test türleri

Black box (kara kutu)

Tester sistem hakkında ön bilgi olmadan, dışarıdan bir saldırgan gibi başlar.

Grey box (gri kutu)

Sınırlı bilgi ve kullanıcı hesabı verilir; yetkilendirme açıkları daha verimli bulunur.

White box (beyaz kutu)

Mimari ve kaynak koda erişimle en derin inceleme yapılır.

Hedefe göre

Dış ağ, iç ağ, web uygulaması, API, mobil uygulama ve kablosuz ağ testleri ayrı kapsamlardır.

03 Kapsam ve kuralları belirlemek

Testten önce yazılı olarak şunlar netleştirilmelidir:

- Hedef listesi: IP aralıkları, alan adları, uygulamalar
- Test zaman penceresi ve kesinti toleransı
- Yazılı yetkilendirme ve iletişim kişileri
- Yasak eylemler (ör. hizmet engelleme, sosyal mühendislik) varsa sınırları
- Hassas veriye erişildiğinde izlenecek prosedür

04 Test öncesi hazırlık listesi

☐ Kapsam ve kurallar yazılı olarak onaylandı	☐ Üretim mi, test ortamı mı hedeflendiği kararlaştırıldı
☐ Kritik sistemlerin yedekleri alındı	☐ İzleme/SOC ekibi bilgilendirildi (veya kör test kararı verildi)
☐ Grey box için test hesapları ve roller hazırlandı	☐ Test kaynak IP adresleri izin listesine alındı
☐ Acil durdurma için iletişim kanalı belirlendi	

05 Test süreci nasıl işler?



06 Raporu nasıl okumalı?

- Yönetici özeti: genel risk durumu ve en önemli birkaç bulgu
- Her bulgu için başlık, risk derecesi, etki, kanıt ve düzeltme önerisi
- Kritik ve yüksek bulgular önce, düşükler planlı düzeltme listesine
- Aynı zafiyetin tekrar etmemesi için kök neden önerileri

Unutmayın: Rapor işin sonu değil başlangıcıdır; her bulguya bir sahip ve hedef tarih atayın, ardından yeniden test yaptırın.

Sızma testi kapsamınızı birlikte belirleyelim Hedeflerinizi dinleyip size uygun test türünü ve kapsamı önerelim.

// İLETİŞİM

Bize ulaşın

İhtiyacınızı ve mevcut durumunuzu paylaşın; size uygun kapsamı ve yol haritasını birlikte belirleyelim. Bilgi formumuzu doldurabilir veya doğrudan bize ulaşabilirsiniz.

Troy Bilgi Teknolojileri Ticaret Limited Şirketi

Atatürk Mah. Vedat Günyol Cad. 44M/2

Ataşehir / İstanbul

T 0-216-575 5222 **E** info@troybilgiteknolojileri.com



Hizmet sayfası ve bilgi formu
için QR kodu okutun