

TEST VE İZLEME

DoS, DDoS Testleri ve Koruma Hizmeti

Hizmetlerinizin yoğun trafik ve kaynak tüketme saldırıları karşısındaki dayanıklılığını kontrollü testlerle ölçüyor, saldırılara karşı koruma mimarisi kurmanıza destek oluyoruz.

**6**

kapsam alanı

5

adımlı yöntem

6

teslim edilen çıktı

// NEDEN ÖNEMLİ?

Neden önemli?

Hizmet dışı bırakma saldırıları, verinizi çalmadan da işinizi durdurabilir. Zayıf noktaları kesinti anında değil önceden bilmek, gerçek dayanıklılığınızı görmenizi sağlar. Koruma tarafında marka bağımsız çalışır, ihtiyacınıza uygun çözümü birlikte seçeriz.



DoS ve DDoS testleri yalnızca yazılı izinle, önceden kararlaştırılan kapsam ve zaman penceresinde, hizmetlerinizi gereksiz riske atmayacak biçimde planlanır. Barındırma, CDN veya bulut gibi üçüncü taraf altyapılarda sağlayıcının test kurallarına uyulur.

// KİMLER İÇİN?

Bu hizmet kimler için uygun?



İnternete açık hizmet veren kuruluşlar (e-ticaret, ödeme, portal)



Kesintinin maliyeti yüksek olan işler



Kampanya veya yoğun dönem öncesinde hazırlanmak isteyenler



Kritik altyapı ve kamu hizmeti sunanlar

// KAPSAM

Neleri kapsıyor?



Saldırı yüzeyi analizi

Hizmetlerinizin internete açık bileşenlerini ve bağımlılıklarını çıkarırız.



Uygulama katmanı testleri

Web uygulama ve API'lerin yoğun istek ve kaynak tüketimi karşısındaki dayanıklılığını ölçeriz.



Ağ ve protokol katmanı

Ağ ve altyapı bileşenlerinin hacimsel ve protokol tabanlı saldırılara dayanıklılığını değerlendiririz.



Kapasite ve ölçeklenme

Darboğazları ve ölçeklenme sınırlarını ortaya çıkarırız.



Koruma mimarisi

CDN, WAF, hız sınırlama ve trafik filtreleme gibi koruma katmanlarını birlikte tasarlarız.



Müdahale prosedürü

Saldırı anında kimin ne yapacağını belirleyen prosedür ve tatbikat hazırlarız.

Saldırgan gibi düşünür, savunmacı gibi inşa ederiz.

// ÇALIŞMA YÖNTEMİ

Nasıl ilerliyoruz?

1

Kapsam ve izinler

Hedefleri, test penceresini ve gerekli izinleri (kendi ve üçüncü taraf sağlayıcılar) netleştiririz.

2

Analiz ve test planı

Saldırı yüzeyini analiz eder, kontrollü bir test planı hazırlarız.

3

Kontrollü test

Planlanan pencerede, kademeli yoğunlukla testi yürütürüz.

4

Raporlama ve önceliklendirme

Bulguları, darboğazları ve önerileri önceliklendirilmiş biçimde sunarız.

5

Koruma uygulaması ve yeniden test

Önlemlerin uygulanmasına destek olur, etkisini yeniden test ederiz.

// ÇIKTILAR

Neler teslim ediyoruz?



Test planı ve kapsam dokümanı



Zayıf nokta ve darboğaz listesi



DDoS müdahale prosedürü



Dayanıklılık test raporu



Koruma mimarisi önerisi



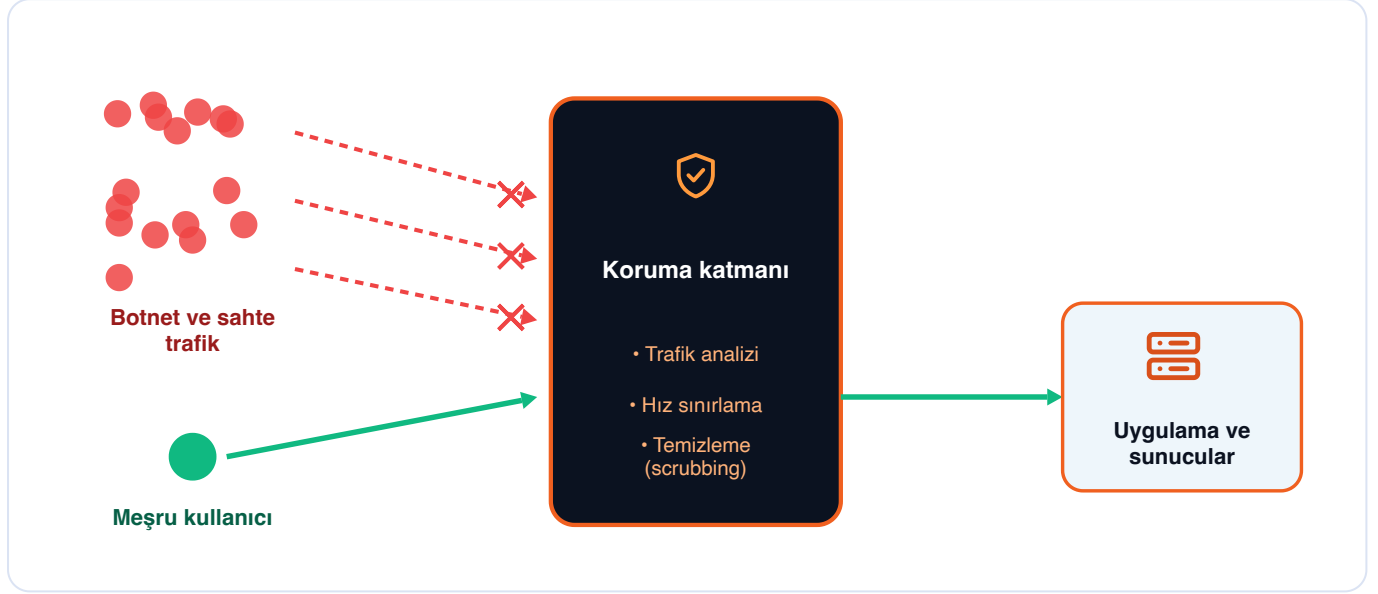
Yeniden test raporu

// GÖRSEL ANLATIM

Konuya özel görseller

DDoS koruması nasıl çalışır?

Koruma katmanı sahte trafiği süzer, meşru kullanıcıların isteklerini hizmete iletir.

**Süzme**

Trafik analizi ve hız sınırlama ile sahte istekler sunucuya ulaşmadan elenir.

Kesintisizlik

Meşru kullanıcılar etkilenmeden hizmete erişmeye devam eder.

Önce test edin

Kontrollü testler, korumanın gerçek yük altında nasıl davrandığını gösterir.

Başlıca saldırı türleri

Testler üç saldırı ailesini kapsar; her birine farklı bir savunma gerekir.

Hacimsel saldırılar (L3/L4)

Bant genişliğini doldurmayı hedefler: UDP/ICMP seli, yansıtma ve büyütme saldırıları.

Protokol saldırıları

Sunucu ve güvenlik duvarı kaynaklarını tüketir: SYN flood, bağlantı tablosu doldurma.

Uygulama katmanı (L7)

Meşru görünen isteklerle uygulamayı yorar: HTTP flood, yavaş istekler, pahalı sorgular.

Farklı saldırı, farklı savunma

Hacimsel saldırı için kapasite ve temizleme; L7 için uygulama düzeyi filtreleme gerekir.

Kapasite planı

Test sonuçları, gerekli bant genişliği ve kaynak planlamasına girdi olur.

Müdahale prosedürü

Saldırı anında kimin ne yapacağı önceden tanımlanır.

// GÖRSEL ÖZET

Hizmete genel bakış

KAPSAM HARİTASI



UYGULAMA DÖNGÜMÜZ



// TEK ÇATI ALTINDA

Diğer hizmetlerimiz

- | | | |
|--|--|--|
|  ISO 27001 Danışmanlığı |  ISO 22301 Danışmanlığı |  ISO 14298 Danışmanlığı |
|  KVKK Uyum Danışmanlığı |  Siber Güvenlik Danışmanlığı |  Risk Yönetimi Danışmanlığı |
|  Sızma Testi |  Düzenli Zafiyet Tarama ve Yönetimi |  SOC / SIEM Kurulumu |
|  Endpoint Security İzleme Hizmeti |  Güvenli Yazılım Geliştirme |  Bilgi Güvenliği Farkındalık Programı |
|  Olay Müdahale Hazırlığı | | |

// 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