DDoS Koruma + WAF Kural Seti Planlama Şablonu (v1.0)

Asset Amacı: Bu şablon; otel ve B2B projelerinde DDoS ve bot riskini azaltmak için CDN'den Origin sunucusuna kadar katmanlı bir koruma planı oluşturmanızı sağlar. Kritik uç noktalar (endpoint) için kural seti tasarımını standartlaştırırken, yanlış bloklama (false-positive) riskini yöneterek SEO ve gerçek kullanıcı deneyimini korur.

Kim Kullanır?: BT yöneticileri, teknik liderler, DevOps ekipleri ve trafik yönetiminden sorumlu teknik SEO paydaşları.

Nasıl Kullanılır? (3 Adım)

1. **Envanter:** Kritik uç noktaları (rezervasyon, login, API) listeleyin ve risk seviyelerini puanlayın.
2. **Konfigürasyon:** WAF kural setlerini "izle-ve-blokla" kademelerine göre planlayın; her profil için hız limitlerini (rate limit) belirleyin.
3. **Operasyon:** KPI ve alarm (alert) planlarını ekleyerek, saldırı anında yapılacakları içeren "runbook" akışını devreye alın.

TEMPLATE: Güvenlik Planlama Şablonu

1) Proje Profili

- **Site Türü:** (Otel / B2B / Diğer)
- **Kritik Akışlar:** Rezervasyon / Login / API / İletişim Formu
- **Edge Katmanı:** CDN Kullanımı (E/H) | Sağlayıcı: _____

2) Kritik Endpoint Envanteri & WAF Planı

Endpoint (URL)	Risk Skoru	Kural Tipi	Aksiyon (İzle/Blok)	Rate Limit (req/sec)
/api/v1/booking	5/5	POST Protection	Blokla	5 req / sec
/login	5/5	Brute Force	Blokla (Captcha)	10 req / min
/search	3/5	Bot Management	İzle	50 req / sec

3) Olay Anı Runbook (Acil Durum Akışı)

- **Tespit:** Trafik türü analizi (Network / L7 / Bot saldırısı?).
- **Sıkılaştırma:** CDN/WAF seviyesinde güvenlik eşiklerini yükselt.
- **SEO Koruma:** Gerçek kullanıcı ve SEO botlarının (Googlebot vb.) bloklanmadığını doğrula.
- **Raporlama:** Saldırı vektörünü raporla ve kalıcı kural setine ekle.

Audit Sheet (Olgunluk Skorlama)

Kriter	Skor (0–5)	Notlar
CDN/Edge Konumlandırma	___	Trafik origin'e gelmeden karşılanıyor mu?
WAF Kural Seti Olgunluğu	___	OWASP Top 10 ve özel kurallar aktif mi?
Rate Limit Kapsamı	___	Endpoint bazlı hız limitleri tanımlı mı?
Bot Yönetimi	___	İyi botlar (SEO) ve kötü botlar ayrışıyor mu?
Log/Alert + KVKK Uyumu	___	Loglar tutuluyor ve kişisel veri gizleniyor mu?

İlk 10 Aksiyon Listesi (Hızlı Koruma)

1. CDN üzerinden IP/Ülke bazlı erişim kısıtlamalarını yapılandır.
2. Rezervasyon motoru POST istekleri için Rate Limit tanımla.
3. WAF üzerinde "Log Only" modunda 48 saatlik trafik analizi yap.
4. Bilinen bot ağlarını (Proxy/VPN/Tor) blokla.
5. SEO botlarını (Google, Bing) "White-list"e al.
6. Origin sunucusuna sadece CDN IP'lerinden erişim izni ver.
7. Kritik formlar için görünmez Captcha/Bot koruması ekle.
8. Saldırı anı bildirimleri için Slack/E-posta alarmlarını kur.
9. Log verilerinin KVKK uyumluluğunu (maskeleme) denetle.
10. Runbook dokümanını tüm teknik ekibe simüle et.

Deliverables

- **Deliverables:** WAF Kural Seti Dokümanı, Rate Limit Profilleri, Olay Anı Runbook, Güvenlik Audit Raporu.