

1

Kontrol et

Kanıt kartı

Sorgu oluştur

Domain veya IP

Shodan verisindeki pasif izleri oku. Tek başına kesin sonuç yazma.

2

example.com

3

Kontrol et

4

Dakika başı 12 canlı sorgu. Sonuçlar kesin kanıt değil, kontrol notudur.

Kendi alan adının dışarıdan görünen izini okumak

Kendi alan adın ya da IP adresin internetten nasıl görünüyor?
Bu masa hedefe tek bir paket göndermeden, Shodan'ın daha önce topladığı kayıtları okur ve gördüğünü yorumdan ayırır.

1 Bu masa ne işe yarar

Bir kurumun internete açık yüzünü görmek için çoğu zaman tarama yapılır. Oysa bunun büyük kısmı zaten açık kayıtlarda durur. Bu masayı bir kuruma saldırır gibi dokunmadan, kendisine ait alan adı ya da IP'nin dışarıdan görünen temel yüzeyini anlaşılır biçimde toplamak için yaptım.

Masada üç sekme var. **Kontrol et** bir alan adı ya da IP için Shodan kayıtlarını getirir. **Kanıt kartı** bu kayıtları bulgu, yorum ve belirsizlik diye ayırır ve rapor metni hazırlar. **Sorgu oluştur** Shodan'da elle kullanabileceğin sorgu taslakları yazar.

Bu masayı yalnızca sana ait ya da incelemek için yazılı izin aldığın varlıklarda kullan. Pasif okuma bile başkasının altyapısını haritalamak için kullanılmamalı.

Birkaç kelime

Shodan	İnternete açık cihaz ve servisleri düzenli tarayıp kaydeden bir arama motoru. Masa bu kayıtları okur, kendisi tarama yapmaz.
Port	Bir sunucudaki servisin kapı numarası. 443 genelde HTTPS, 22 genelde SSH.
Banner	Bir servisin bağlanınca kendini tanıttığı kısa metin. Ürün adı ve sürüm buradan okunur.
ASN	Bir IP bloğunu yöneten ağın numarası. Hangi sağlayıcıda olduğunu söyler.
TLS	HTTPS bağlantısını şifreleyen protokol. Eski sürümleri (TLS 1.0, 1.1) kontrol gerektirir.
Pivot	Bir izden (favicon özeti, sertifika parmak izi) benzer servisleri bulmaya geçmek.

2 Kontrol et sekmesi

1

Kontrol etKanıt kartıSorgu oluştur

2

Domain veya IP
Shodan verisindeki pasif izleri oku. Tek başına kesin sonuç yazma.
example.com

3

Kontrol et

4

Dakika başı 12 canlı sorgu. Sonuçlar kesin kanıt değil, kontrol notudur.

Kontrol et sekmesi, alan adı yazıldı, sorgu henüz gönderilmedi.

1

Sekmeler

Sayfa Kontrol et sekmesiyle açılır. Kanıt kartı sekmesi ancak bir sorgudan sonra dolar.

2

Alan adı ya da IP

example.com ya da bir IPv4 adresi yaz. Başına https:// eklersen ya da sonuna yol yazarsan masa bunları temizler. IPv6 kabul edilmez.

3

Kontrol et

Biçim uymazsa uyarı çıkar ve sorgu gönderilmez. Uyarsa birkaç saniyede sonuç aynı sayfada açılır.

4

Sorgu sınırı

Dakikada en fazla 12 canlı sorgu. Sonuçlar kesin kanıt değil, kontrol notudur.

Canlı sitede example.com için normal sorguyu denedim. İnsan doğrulaması geçici olarak kullanılamıyor yanıtı geldi. Bu kontrolü aşmadım ve sonuç ekranı üretmedim. Aşağıdaki alanları masanın koduna bakarak anlatıyorum.

3 Sonucu okumak

Sorgu çalışınca Türkçe sayfada sonuç dört parça halinde gelir.

Özet kutusu

Hedef, tür, IP, ASN, kurum, ülke, görünen portlar ve Shodan'ın son gözlem tarihi. Görünmeyen alanlarda Yok / görünmedi yazar.

Servis izleri

Her port için bir kart var. Kartta port ve protokol, ürün ve sürüm, hostname, HTTP başlığı ve sunucu adı, TLS sürümü, gözlem tarihi ve en fazla dört HTTP başlığı yer alır. Eski TLS görülürse kart Kontrol gerekli etiketi alır, yoksa Görünür iz.

TLS ve sertifika

TLS sürümü, sertifikadaki ad (CN), diğer adlar (SAN), sertifikanın bitiş tarihi ve HTTP/2 bilgisi.

Benzer servis izleri

Favicon özeti, başlık özeti, sertifika parmak izi ve sayfa başlığı. Bunlar kendi envanterinde aynı izi taşıyan başka servis var mı diye bakmak içindir.

İngilizce sayfa

İngilizce sürüm daha sade. Özet kutusu ve servis izleri var, TLS ve benzer iz panelleri yok. Servis kartında HTTP başlık listesi de yer almaz.

Kanıt kartı sekmesi

Sorgudan sonra bu sekmede bir özet kartı ve her servis için bir kart çıkar (en fazla sekiz servis). Her kart aynı yedi satırı taşır. Bunlar bulgu, kaynak, kanıt, yorum, belirsizlik, güvenli öneri ve rapor cümlesidir. Altında Markdown rapor metni ve **Markdown kopyala** düğmesi durur.

Rapor cümleleri bilerek temkinli yazıldı. "Zafiyet var" demez, "servis izi görünüyor, envanterle doğrulanmalı" der. Bir ürün adı ya da sürüm, tek başına açık olduğu anlamına gelmez.

4 Sorgu oluştur sekmesi

Savunma odaklı Shodan sorgusu üret.

Bu bölüm sorguyu çalıştırmaz; izimli envanter ve raporlama dili için sorgu taslağı hazırlar.

1 Alan

hostname

2 Değer

portal.example.org

Kopyala

3 Üretilen sorgu

hostname:portal.example.org

Domain görünürlüğü

hostname:example.com

Kurum adı görünürlüğü

org:"Example"

Sorgu oluştur sekmesi. Bu bölüm hiçbir şey göndermez, yalnızca sorgu metni yazar.

1 Alan

hostname, domain, org, asn, port, product, ssl.cert.subject.cn, ssl.version, http.title, http.favicon.hash ve cloud.provider arasından seç.

2 Değer

Aranacak değeri yaz. Değerde boşluk varsa tırnak gerekir. Türkçe sayfa tırnağı kendisi ekler, İngilizce sayfada elle eklemelisin.

3 Üretilen sorgu

Shodan'a elle yapıştırılabileceğin sorgu. Türkçe sayfada altında beş hazır örnek ve bir Kopyala düğmesi de var.

Sorgunun altında dört kutu seçtiğin alanı açıklar. Kutular bu sorgunun neyi gösterdiğini, neyi göstermediğini, hangi durumda kullanıldığını ve rapora nasıl yazıldığını anlatır. Sekmenin en altındaki **Türkiye görünürlük eğilimi** paneli, Türkiye'deki kayıtların port, ürün, TLS sürümü ve bulut sağlayıcı dağılımını sayılarla gösterir. Tek tek hedef listelemez.

5 Verin nereye gider

Gönderilen	Yazdığın alan adı ya da IP, CSINT'in Cloudflare üzerindeki Shodan sunucusuna gider.
Sorulan	Sunucu Shodan API'sine sorar. IP için o adresin kaydı, alan adı için DNS kaydı ve o ada bağlı servisler istenir. Hedefe hiçbir paket gönderilmez.
Bot kontrolü	Her sorgudan önce Cloudflare Turnstile görünmeden çalışır.
Önbellek	Sonuç sunucuda birkaç dakika saklanır. Aynı hedefi hemen tekrar sorarsan aynı cevap gelebilir.
Tarayıcıda kalan	Kanıt kartları, rapor metni ve sorgu taslakları tarayıcında oluşur.

6 Neyi yapmaz

- × Tarama yapmaz, porta bağlanmaz, parola denemez.
- × Zafiyet bulmaz. Eski bir sürüm adı bile yalnızca kontrol edilecek bir izdir.
- × Eksiksiz varlık envanteri değildir. Shodan'ın görmediği servis yok demek değildir.
- × Kayıtlar Shodan'ın gözlem tarihine bağlıdır. Servis kapanmış ya da değişmiş olabilir.
- × Bir hostun sana ait olduğunu kanıtlamaz. Her bulguyu kendi envanterinle karşılaştır.

Eski DNS ve arama motoru kayıtlarını aktif varlık gibi okuma. Bir bulguyu rapora yazmadan önce tarihine ve ikinci bir kaynağa bakarım.