



Araştırma dosyaları

Çalışmalar

E-kütüphane

Hakkında

TR

EN



IOC masası

IOC Masası

IP, domain, hash veya URL yapıştır. Açık kaynaklar ne diyor, ne eksik, notuna ne yazabilirsin. Hepsini burada gör.

Yalnızca canlı açık kaynaklar. Sorgu CSINT sunucusu üzerinden gider.

01 Yapıştır

02 Kontrol et

03 Oku

04 Kopyala

Kontrol etmek istediğin gösterge

IOC: IP, domain, dosya özeti (hash) veya web adresi.

Tehdit istihbaratı akışı nasıl kuruldu

Tehdit istihbaratı akışı, açık kaynak güvenlik kayıtlarını düzenli aralıklarla toplayan, tekrarları ayıklayan ve önemli değişiklikleri öne çıkaran bir arka plan servisi. Kendine ait bir sayfası yok. Bu kılavuzda akışın nasıl çalıştığını ve çıktısının sitede nerede görüldüğünü anlatıyorum.

1 Bu bir sayfa değil, bir akış

Açıklanan her yeni zafiyeti, her üretici duyurusunu ve her yeni gösterge listesini elle takip etmek mümkün değil. Aynı olay birkaç kaynakta farklı adla da geçebiliyor. Bu akışı bunun için kurdum. Kaynakları okuyor, aynı biçime çeviriyor, tekrarları birleştiriyor ve neyin gerçekten değiştiğini kaydediyor.

Akış Cloudflare üzerinde çalışan bir Worker. Ziyaretçi bir şey tetiklemiyor. Worker zamanlayıcıyla kendisi çalışıyor ve sonucu bir veritabanına yazıyor. Sitedeki sayfalar bu sonucu okuyor.

Akışın kendine ait bir sayfası yok. Çıktısı Tehdit aktörleri sayfasındaki canlı akış bölümünde, Android tehditleri sayfasında ve kaynak değişiklikleri sayfasında görünüyor. Bu kılavuzdaki ekran görüntüleri bu yüzden o sayfalardan ve IOC masasından alındı.

Birkaç kelime

CVE	Açıklanan bir güvenlik açığına verilen standart numara.
KEV	CISA'nın, gerçekte istismar edildiği bilinen açıklar listesi.
EPSS	FIRST'ün, bir açığın yakında istismar edilme olasılığı için yayımladığı tahmin.
CVSS	Bir açığın teknik ağırlığını 0 ile 10 arasında gösteren puan.
IOC	Bir saldırıyı işaret eden iz. IP adresi, alan adı, dosya özeti ya da adres olabilir.

2 Kaynaklar ve zamanlama

CISA KEV	İstismar edildiği bilinen açıklar. Ana adres açılmazsa CISA'nın GitHub kopyası okunur.
NVD	ABD ulusal zafiyet veritabanı. Her çalışmada en fazla 50 kayıt.
FIRST EPSS	Açıkların istismar olasılığı tahmini. Ayrı bir kayıt olarak değil, CVE kayıtlarına ek bilgi olarak okunur.
CISA CSAF	CISA'nın makine okunur güvenlik duyuruları, GitHub deposundaki değişikliklerden.
Microsoft Security	Microsoft güvenlik blogunun RSS akışı. Göstergeler yalnız bu ve bir sonraki kaynaktan çıkarılır.
Google ve Mandiant	Google ve Mandiant tehdit istihbaratı blogunun RSS akışı.

Her 5 dakikada	Her gün 05:00 UTC	Sayfa açılınca
Kaynaklar okunur, kayıtlar düzenlenir ve veritabanına yazılır.	Öncelikler yeniden hesaplanır ve günlük briefing üretilir.	Tarayıcı yalnız hazır sonucu okur. Kaynaklara ziyaretçi adına istek gitmez.

Her kaynak için en fazla 20 saniye beklenir ve en fazla 2,5 MB okunur. NVD için bu sınır 4 MB. Bir kaynak o an cevap vermezse diğerleri çalışmaya devam eder.

3 Düzenleme, tekrar ve değişiklik

1 Aynı biçim

Her kaynak kendi biçiminden ortak bir kayda çevrilir. Başlık 320, özet 1400 karakterle sınırlanır. Tarihler tek biçime getirilir.

2 Sabit kimlik

Kaydın kimliği kaynak adı ve kaynaktaki numarasından SHA-256 ile üretilir. Aynı kayıt tekrar gelince yeni bir kayıt açılmaz.

3 Yalnız değişince güncelleme

Kaydın içeriğinden ayrıca bir özet alınır. Özet değişmediyse hiçbir şey yazılmaz. Değiştiyse kayıt güncellenir ve her sürüm ayrı bir tabloda saklanır.

4 Gösterge birleştirme

Aynı IP, alan adı ya da dosya özeti farklı kaynaklarda geçiyorsa tek göstergede toplanır. İlk ve son görölme tarihi, kaynaklar ve ilgili CVE'ler birleşir.

5 Önemli değişiklik

Göstergenin eklenmesi ya da kalkması, açığın KEV'e girmesi, EPSS'in yükselmesi, etkilenen ürünlerin, çözüm önerisinin ya da CVSS'in değişmesi ve duyurunun geri çekilmesi ayrıca kaydedilir. Bu kayıtlar 180 gün tutulur.

4 Öncelik puanı

Her CVE için 0 ile 100 arasında bir puan hesaplanıyor. Formül koda açık yazılı. Gizli bir model ya da yapay zeka kararı yok.

KEV'de ya da aktif
istismar +55

Fidye yazılımında
kullanıldığı biliniyor +20

EPSS 0,5 ve üstü, 0,1
ve üstü, 0,01 ve üstü +20, +12, +5

CVSS 9 ve üstü, 7 ve
üstü, 4 ve üstü +15, +10, +5

Son 7 gün içinde
yayımlandı +5

Seviye 70 ve üstü acil, 50 ve üstü bugün, 10 ve üstü izle, altı düşük.

Puan bir sıralama yardımıdır. Senin sistemlerinde o açığın olup olmadığını bilmez. Son risk kararı, saldırgan ataması ya da otomatik müdahale kararı değildir.

5 Sitede nerede görünür

✓ Yeni olayları ve duyuruları göster

1

Canlı tehdit akışı

2

Tüm olaylar

Tüm seviyeler

Tüm sektörler

Tüm kaynaklar

Tüm aktörler

3

Canlı, Şimdi güncellendi

CVE-2026-96342

Missing Authorization vulnerability in Amauri.IO WPMobile.App wpappninja al...

Orta

NVD

30 Eyl 2026 14:16

CVE-2026-76992

The CODESYS Gateway Client allocates memory based on a size field in a gate...

Yüksek

NVD

30 Eyl 2026 14:16

CVE-2026-13720

An Editor can set file-provisioning metadata (the grafana.app/managedBy, gr...

Orta

NVD

30 Eyl 2026 14:16

Canlı sitedeki tehdit akışı. Kaynaklardan gelen gerçek olaylar filtrelerin altında listeleniyor. Başlıklar kaynağın kendi dilinde bırakılmış.

1 Akışın kaynağı

Bölüm hangi kaynakların ne sıklıkla kontrol edildiğini yazıyor.

2 Süzgeçler

Olay türü, kaynak, önem, aktör ve sektöre göre süzme. Süzme Worker'a sorgu olarak gider.

3 Durum

Akış alınamadığında bunu açıkça söyler ve eski bir listeyi yeniymiş gibi göstermez. Tarayıcı listeyi dakikada bir yeniler.

Worker dışarıya akış, panel özeti, değişiklikler, tek olay ve günlük brifing için okuma uçları açıyor. Brifing her gün İstanbul tarihine göre bir kez üretilip saklanıyor. İçinde son 24 saatin sayıları, öne çıkan 5 olay, 5 CVE, 10 gösterge, 6 sektör ve en fazla 5 çözüm önerisi var. Bugün sitede brifingi doğrudan gösteren bir sayfa yok.

6 Bir sonraki adım, IOC masası

Akış genel resmi veriyor. Tek bir göstergiyi sormak istediğinde IOC masasına geçiyorsun. Masa ayrı bir Worker kullanıyor ve yalnız sen sorduğunda çalışıyor.

