

Mobil uygulama inceleme ve maruziyet analizi

Mobile Exposure Graph

APK yapısını çalıştırmadan incele; izin, kod, altyapı izi, bulgu ve kanıt konumunu tek ilişki grafiğinde gör. İki sürümü karşılaştır ve hash-bağlı kanıt paketi üret.

Doğru ürün sınırı

Bu ilk sürüm EDR değildir. Cihaz ajanı, canlı telemetri, otomatik engelleme veya kötü amaçlı yazılım kararı üretmez. Dosya tarayıcıda kalır ve çalıştırılmaz.

01 Yerel alım

02 Sınırlı statik analiz

03 Kanıt bağlantısı

04 Graph + diff

05 Doğrulanabilir çıktı

İncelenecek APK

Güncel veya şüpheli sürüm. Sonuç grafiğinin ana dosyasıdır.

1

APK seç

Dosyayı seç veya bu alana bırak

APK, en fazla 100 MB, sunucuya gönderilmez

Henüz dosya seçilmedi

Referans APK (isteğe bağlı)

Daha eski ya da bilinen sürüm. Yalnız fark analizi için kullanılır.

2

Referans APK seç

Dosyayı seç veya bu alana bırak

APK, en fazla 100 MB, sunucuya gönderilmez

Henüz dosya seçilmedi

3

Tümünü temizle

Mobile Exposure Graph ile bir APK'yı çalıştırmadan incelemek

Bir Android uygulamasının dosyasını açıyorum ama çalıştırmıyorum. İzinleri, kod izlerini ve adresleri bir grafikte, her bulguyu dosyadaki yerile birlikte görüyorum.

1 Bu araç ne işe yarar

APK incelemesi genelde uzun bir tabloyla biter. Ben bir iznin, bir adresin ya da bir kod izinin hangi dosyada durduğunu aynı yerde görmek istedim. Bu araç her bulguyu kanıtına bağlar. İki sürüm verirsен aradaki farkı da gösterir.

Her şey tarayıcında olur. APK sunucuya gitmez ve hiçbir zaman çalıştırılmaz. Araç dosyanın içeriğini okur, o kadar.

Birkaç kelime

APK	Android uygulamasının kurulum dosyası. Aslında içinde başka dosyalar olan bir ZIP'tir.
Manifest	AndroidManifest.xml. Uygulamanın adını, sürümünü, istediği izinleri ve bileşenlerini yazan dosya.
İzin	Uygulamanın telefondan istediği kamera, internet ya da konum gibi bir yetki.
DEX	Uygulamanın Java ya da Kotlin kodunun derlenmiş hali.
Native kütüphane	APK içindeki .so dosyası. Doğrudan işlemci için derlenmiş koddur.
Cleartext	Şifresiz ağ trafiği. Adres http ile başlar, https ile değil.

2 Dosyayı seçmek

Gereken	Bir .apk dosyası, en fazla 100 MB.
İsteğe bağlı	Karşılaştırma için aynı uygulamanın eski ya da bilinen bir sürümü.
Hesap	Gerekmez.
Veriler nerede	APK tarayıcında ayrı bir işçi süreçte (worker) okunur. Sunucuya gönderilmez.

Mobile Exposure Graph

APK yapısını çalıştırmadan incele; izin, kod, altyapı izi, bulgu ve kanıt konumunu tek ilişki grafiğinde gör. İki sürümü karşılaştı ve hash-bağlı kanıt paketi üret.

Doğru ürün sınırı

Bu ilk sürüm EDR değildir. Cihaz ajanı, canlı telemetri, otomatik engelleme veya kötü amaçlı yazılım kararı üretmez. Dosya tarayıcıda kalır ve çalıştırılmaz.

01 Yerel alım

02 Sınırlı statik analiz

03 Kanıt bağlantısı

04 Graph + diff

05 Doğrulanabilir çıktı

İncelenen APK

Güncel veya şüpheli sürüm. Sonuç grafiğinin ana dosyasıdır.

1

APK seç

Dosyayı seç veya bu alana bırak

APK, en fazla 100 MB, sunucuya gönderilmez

Henüz dosya seçilmedi

3

Tümünü temizle

Referans APK (isteğe bağlı)

Daha eski ya da bilinen sürüm. Yalnız fark analizi için kullanılır.

2

Referans APK seç

Dosyayı seç veya bu alana bırak

APK, en fazla 100 MB, sunucuya gönderilmez

Henüz dosya seçilmedi

Dosya alanları. Sitede örnek APK yok; iki alan da kendi dosyanı bekler.

1

İncelenen APK

Şüphelendiğin ya da güncel olan sürüm. Grafik bu dosyaya göre çizilir.

2

Referans APK

İstersen daha eski ya da bildiğin bir sürüm ekle. Yalnızca farkı bulmak için kullanılır.

3

Temizle

Tümünü temizle iki alanı ve sonucu sıfırlar. Dosya adı ve Analiz tamamlandı yazısı çıkınca sonuç sayfanın altında açılır.

3 Özet ve inceleme kuyruğu

Bu ve sonraki bölümlerde ekran görüntüsü yok. Sitede örnek APK yayımlamıyorum ve sentetik bir dosyanın sonucunu göstermek yerine ekrandaki parçaları anlatıyorum.

Bulgu sayısı

Toplam bulgu ve altında düşük ve bilgi düzeyindekilerin sayısı.

Yüksek ve orta

Önce bakılacaklar. Orta düzey bulgu uygulamanın amacını bilmeden yorumlanamaz.

Kapsam

Aracın dosyanın ne kadarını okuyabildiği. *Sınırlı* yazıyorsa bir alan eksik kaldı ve eksik bilgi güvenli sayılmadı.

Bir bulgu seç	Kuyruktaki her kart bir bulgudur. İlk kart seçili gelir.
Önem derecesine bak	Yüksek, orta, düşük ya da bilgi.
Kuyruğun altında seçili bulgunun kanıtı durur.	
Güven temeli	Bulgunun neye dayandığı ve yüzdesi. Manifestten okunanlar kesin kurala (deterministic) dayanır. Metin taramasından gelenler bir tahmindir (heuristic).
Konum ve değer	İz hangi dosyada ve hangi değerle geçiyor. Bu konumu kendi aracınla da açıp kontrol edebilirsin.
Yorum sınırı	Bu bulgunun neyi kanıtlamadığı. Bir metin izi, bağlantının gerçekten kurulduğu anlamına gelmez.

4 Kanıt grafiği

Grafikteki katmanlar soldan sağa dosya, kimlik, yüzey, kod, altyapı izleri, bulgular ve kanıttır. Grafik geniştir, sağdaki katmanları görmek için yana kaydırırsın. Bir düğüme basınca ilişkili çizgiler vurgulanır.

Grafiğin altında seçili düğümün adı ve doğrudan ilişkileri yazar. Bu ilişkiler düğümün hangi dosyadan çıktığını ve hangi kanıtla desteklendiğini gösterir. Tüm ilişki tablosu da oradan açılır.

5 İki sürümü karşılaştırmak

İzinler	Referanstan adaya eklenen ya da kalkan izinler. Artı eklenen, eksi kaldırılan öğeyi gösterir.
Altyapı izleri	Kodda bulunan alan adı, IP ve adreslerdeki ekleme ve çıkarmalar.
İmza kayıtları	META-INF altındaki imza dosyasının parmak izindeki değişiklik. Araç imzanın geçerli olup olmadığını kontrol etmez, yalnızca farkı gösterir.

Bir değişiklik kendiliğinden risk ya da onay demek değildir. Yeni bir izin, yeni bir özelliğin normal sonucu olabilir.

6 Kanıt paketini almak

ZIP'i indir

İçinde rapor (JSON ve Markdown), grafik, varsa fark dosyası ve her dosyanın SHA-256 değerini tutan bir manifest var. Orijinal APK pakete girmez.

Paketi doğrula

Daha önce indirdiğin bir ZIP'i seç. Dosya adları, boyutlar ve SHA-256 değerleri cihazında kontrol edilir.

Doğrulama kartı bir APK incelendikten sonra rapor bölümünde görünür. Araç doğrulama sayfasında F-Droid istemcisinin (org.fdroid.fdroid 1.23.2) gerçek kanıt ZIP'i ve SHA-256 değeri yayımlı; o dosyayı bu kartla kontrol edebilirsin.

Paket SHA-256 ile birbirine bağlıdır ama dijital olarak imzalı değildir. Dosyaların değişmediğini gösterir, kimin ürettiğini göstermez.

7 Neyi yapmaz

- × Uygulamayı çalıştırmaz. Bir iznin gerçekten kullanıldığını kanıtlamaz.
- × Zararlı yazılım kararı vermez. Bulgu çıkmaması dosyanın güvenli olduğu anlamına gelmez.
- × Telefona ajan kurmaz, canlı izleme ya da engelleme yapmaz.
- × Daha derin inceleme için sayfanın altındaki Dosya ve belge sandbox bağlantısını kullan. Oradaki izole analiz ayrı onayla çalışır; bu sayfa oraya kendiliğinden dosya göndermez.
- × Metin taraması sınırlıdır. Çok büyük dosyalarda bir kısmı okunmayabilir; bu durumda kapsam Sınırlı yazar.