



Araştırma dosyaları

Çalışmalar

E-kütüphane

Hakkında

TR

EN



n8n güvenlik takibi

n8n Workflow Güvenlik Takibi

Bir n8n dosyası seç. Araç hangi parçaları kullandığını gösterir, sürümünü bildiğimiz parçaları açık güvenlik kayıtlarında kontrol eder ve daha sonra dosyada önemli bir değişiklik olursa bunu ayrı gösterir.

Dosyanın kendisi kaydedilmez. Bir sürümü bilmiyorsak tahmin etmeyiz; ekranda 'bilinmiyor' yazar.

01 Dosyanı seç

02 Sürümü yaz

03 Sorunları gör

04 Değişikliği izle

İlk adım

n8n dosyanı seç

Dosya yalnızca bu tarayıcıda açılır. Araç önce içinde hangi parçaların bulunduğunu gösterir.

n8n dosyası

Kullandığın n8n sürümü

Exposure Watch nasıl kuruldu

Bir n8n workflow dosyasını tarayıcında okuyorum, içinden kısa bir parça listesi çıkarıyorum ve yalnızca bu listeyi saklıyorum. Sonra tam sürümü bilinen paketleri açık güvenlik kayıtlarıyla eşleştiriyor, yeni bir dosya geldiğinde önemli bir değişiklik olup olmadığına bakıyorum.

1 Hangi boşluğu dolduruyor

Bir workflow'u bir kez incelemek, o günkü dosyayı anlatır. Ama sonra da üç şeyi bilmek gerekir. Birincisi workflow'un hangi n8n ve paket sürümlerine dayandığı. İkincisi yeni yayımlanan bir güvenlik kaydının tam olarak senin sürümünü etkileyip etkilemediği. Üçüncüsü daha önce incelediğin yapının sonraki dışa aktarmada değişip değişmediği.

Exposure Watch bu üç soruya bakar. Workflow'u çalıştırmaz, canlı sistemine bağlanmaz. Yalnızca dosyadan çıkan yapıyı ve senin yazdığın sürümleri kullanır.



maruziyet-takibi sayfası. Dört adım, aracın yaptığı işin kısa özeti.

1 Dosyanı seç

n8n'den dışa aktardığın JSON dosyası tarayıcıda açılır.

2 Sürümü yaz

Dosya, kurulu sürümleri içermez. n8n sürümünü ve bildiğin paket sürümlerini sen yazarsın.

3 Sorunları gör

Tam sürümü bilinen paketler OSV kayıtlarıyla eşleştirilir.

4 Değişikliği izle

Yeni bir dosya ya da yeni bir kayıt çıktığında uyarı oluşur.

2 Nerede ne çalışır

	Tarayıcı	Worker	D1	OSV	Cron
	JSON'u okur, hassas alanları atar, kısa bir liste üretir.	Girişi doğrular, listeyi kontrol eder, sahibine bağlı kayıt yazar.	Liste, uyarılar ve değişiklik geçmişi burada durur.	Yalnızca paket adı ve tam sürümle sorgulanır.	Belli aralıklarla aynı kontrolü tekrarlar ve yeni uyarı açar.
Hesap	Dosyada bulunanları görmek için gerekmez. Kaydetmek, düzenli kontrol ve uyarı geçmişi için CSINT topluluk hesabı gerekir.				
Giriş	Topluluk oturumu, kısa ömürlü bir kimliğe çevrilir. Worker her kaydı bu kimliğin sahibine bağlar.				
Kaydedilen	Adım ve paket türleri, doğrulanmış sürümler, hesap türleri, dışarıya bağlanılan alan adları, yetenekler ve bir yapı özeti.				
Kaydedilmeyen	Ham JSON, promptlar, adım adları, credential kimlikleri, webhook yolları ve serbest parametre değerleri.				
Dış istek	Worker yalnızca OSV'ye paket adı ve sürüm gönderir. Workflow içeriği gitmez.				

Birkaç kelime

Manifest	Dosyadan çıkarılan kısa parça listesi. Saklanan tek şey bu.
OSV	Açık kaynak paketler için herkese açık güvenlik kaydı veritabanı. npm ve GitHub kayıtlarını içerir.
Yapı özeti	Riskle ilgili yapıdan üretilen bir kod. Yapı değişirse kod da değişir.
Kapsam boşluğu	Sürümü bilinmeyen paket. Etkilenmiyor sayılmaz, bilinmiyor olarak kalır.

3 Dosyayı seçmek

İlk adım

n8n dosyası seç

Dosya yalnızca bu tarayıcıda açılır. Araç önce içinde hangi parçaların bulunduğunu gösterir.

1

n8n dosyası

JSON dosyası seç

2

Kullandığın n8n sürümü

Örn. 2.21.5

n8n dosyası bu bilgiyi içermez. Ayarlar ya da kurulum ekranındaki sürümü yaz.

3

Dosyada bulunanları giriş yapmadan görebilirsin. Kaydetmek, düzenli kontrol ve uyarı geçmişi için hesap gerekir.

Eski kurum ve site takiplerini aç

İlk adım paneli. Giriş yapmadan da dosyayı okutabilirsin.

1 n8n dosyası

JSON dosyasını seç. Dosya bu tarayıcıda okunur. Ardından dosyada bulunan adım, paket, bağlanmış site ve hesap türü sayıları çıkar.

2 n8n sürümü

Ayarlar ya da kurulum ekranındaki sürümü yaz. Bu sürüm yalnızca çekirdek n8n paketine uygulanır.

3 Hesap notu

Görmek serbest. Takibi kaydetmek, tekrar kontrol ve uyarı geçmişi için giriş gerekir.

Paket sürümlerini n8n dosyası yazmaz. n8n-nodes-base gibi paketlerin sürümü, n8n'in kendi sürümünden farklı olabilir. Bilmiyorsan boş bırak. Araç tahmin etmez, o paketi kapsam boşluğu olarak gösterir.

Dosya okununca panelde adım, paket, bağlanılan site ve hesap türü sayıları, paketlerin sürüm durumu ve adım türlerinden çıkarılan yetenekler görünür. Sürümünü yazmadığın paketler "bilinmiyor" olarak kalır ve OSV kontrolüne girmez. Sitede örnek bir workflow dosyası yayımlamadığım için bu kısmın ekran görüntüsü yok.

Kayıt olmadan önce ekranda sunucuya gidecek listenin ne olduğu da yazmaz. Bu noktaya kadar hiçbir şey gönderilmedi.

4 Uyarılar nasıl oluşur

İki tür uyarı var. Birincisi bilinen bir güvenlik sorunu. Yazdığın tam sürüm için OSV'de bir kayıt varsa açılır. İkincisi dosya değişikliği. Yeni yüklediğin dosyanın yapı özeti kayıtlı olandan farklıysa açılır.

Açık	Yeni uyarı. Henüz bakılmadı.
İnceleniyor	Sen "İnceliyorum" dedin.
Çözüldü	Sorun giderildi ya da artık bu sürümü etkilemiyor.
Eşleşme değil	Kaydın bu dosyayla ilgisi olmadığına sen karar verdin.

Aynı güvenlik kaydı bir kez eklenir, sonraki kontrollerde güncellenir. Bir kaydın kapanması için OSV'den tam yanıt gelmesi gerekir. Eksik ya da kesilmiş bir yanıt yeni uyarı ekleyebilir ama eski bir uyarıyı asla kapatmaz. Aynı dosyayı tekrar yüklersen değişiklik kaydı oluşmaz.

5 Neden böyle kurdum

Ham dosyayı saklamamak

Bir n8n dosyası çoğu zaman promptlar, iç adresler ve müşteriye özel mantık taşır. Sürüm takibi için bunların hiçbirine gerek yok. Bu yüzden sunucuya yalnızca kısa liste gider ve Worker listede tanımadığı bir alan görürse kaydı reddeder.

Sürümü tahmin etmemek

Sürüm yoksa eşleşme de yoktur. Bilinmeyen bir sürümü etkilenmiyor saymak, yanlış bir güven verir. Bu yüzden boşluk ekranda açıkça durur.

Dış servise nazik davranmak

Worker OSV'ye aynı anda en fazla altı bağlantı açar. Elle yapılan bir kontrolde en fazla 40 kaydın ayrıntısını okur, zamanlanmış her çalışma da 40 okumalık ortak bir sınırı paylaşır.

6 Sınırlar

- ✗ Workflow çalıştırılmaz. Modelin çalışırken ne yaptığına bakılmaz.
- ✗ Temiz bir OSV sonucu bir güvenlik kararı değildir. Henüz yayımlanmamış açıkları gösteremez.
- ✗ Bir kaydın görünmesi saldırıya uğradığın anlamına gelmez. Kaynağı aç, sürümünü doğrula, güncelleme notlarını oku.
- ✗ Credential'ların gerçek yetkisini ve canlı ortamın ayarlarını göremez.
- ✗ Sonuç, senin yazdığın sürümler kadar doğrudur.