

## Yerel sürüm provası

1

DENEYSEL AÇIK LAB, ÜCRETLİ TESLİM İNCELEMESİNE DAHİL DEĞİL

## İş akışı değişikliğini dış sisteme dokunmadan prova et

Bu deneysel açık laboratuvarındaki yerel komut satırı aracı, desteklenen başlangıç ve aday iş akışlarını ayrı

Docker ortamlarında sentetik test verileriyle çalıştırır. HTTP eylemleri yalnız yerel yakalama servisine gider.

Bu ekran oluşan üç dosyanın parmak izlerini tarayıcıda doğrular ve farkları okunabilir hale getirir.

2

## Ne kanıtlanır?

Gözlemlendi demek, dönüştürülmüş sentetik isteğin yerel yakalama servisine ulaştığı anlamına gelir. Düğüm çalışma sırası, insan onayları, yeniden deneme ve döngü davranışı, canlı sistem güvenliği veya penetrasyon testi sonucu kanıtlanmaz. Son sürüm kararı insandadır.

# n8n AI güvenlik regresyon kapısı nasıl kuruldu

Bir n8n workflow'u değişince, korunması gereken bir güvenlik davranışı da bozulabilir. Bu kapı, değişikliği canlı sisteme dokunmadan yerel ve kapalı bir ortamda deniyor ve ne gözlemlendiğini sınırlarıyla birlikte yazıyor.

## 1 Bu çalışma nedir

Statik inceleme bir dosyada neyin yazdığını gösterir. Ama bir değişiklikten sonra imzasız isteğin yine reddedilip reddedilmediğini ya da onay beklemeden dışarıya bir eylem gidip gitmediğini göstermez. Ben bunu yayından önce, gerçek sistemlere hiç dokunmadan görmek istedim.

Sonuç, n8n-ai-agent-security-lab adlı açık kaynak bir komut satırı projesi oldu. MIT lisanslı, Node.js 20 ile çalışıyor ve ek paket kurulumu istemiyor. Workflow dosyaları bilgisayarında kalır. Araç bir AI servisine istek göndermez.

|                            |                                                                                                                                    |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>Statik denetim</b>      | Dışa aktarılan workflow'daki riskli yolları raporlar. Hiçbir şey çalıştırmaz.                                                      |
| <b>Regresyon kapısı</b>    | Bir sözleşme dosyasındaki sentetik istekleri izole bir staging webhook'una gönderir ve değişmemesi gereken davranışı kontrol eder. |
| <b>Yerel sürüm provası</b> | Baseline ve candidate sürümleri ayrı Docker ortamlarında çalıştırır ve eylem farkını kaydeder.                                     |
| <b>GitHub PR kapısı</b>    | Her pull request'te depodaki workflow dosyalarını çalıştırmadan inceler ve kanıt dosyaları bırakır.                                |

### Birkaç kelime

|                        |                                                                                              |
|------------------------|----------------------------------------------------------------------------------------------|
| <b>Regresyon</b>       | Daha önce doğru çalışan bir davranışın yeni bir değişiklik ile bozulması.                    |
| <b>Baseline</b>        | Bugün kullanılan, daha önce onaylanmış workflow sürümü.                                      |
| <b>Candidate</b>       | Yayına alınmak istenen yeni sürüm.                                                           |
| <b>Staging</b>         | Gerçek sistemlere bağlı olmayan deneme ortamı.                                               |
| <b>Fixture</b>         | Test için hazırlanmış, gerçek veri içermeyen örnek girdi.                                    |
| <b>Sözleşme</b>        | Staging workflow'unun hangi isteğe nasıl cevap vermesi gerektiğini yazan küçük JSON dosyası. |
| <b>Capture servisi</b> | Provada HTTP isteklerini gerçek hedef yerine kabul eden yerel dinleyici.                     |

## 2 Ne nerede çalışır

Bütün çalıştırma senin bilgisayarında olur. CSINT sitesi yalnızca provanın ürettiği üç dosyayı tarayıcı belleğinde doğrular. Site Docker ya da n8n çalıştırmaz.

|                                                                         |                                                             |                                              |                                                  |                                                     |                            |
|-------------------------------------------------------------------------|-------------------------------------------------------------|----------------------------------------------|--------------------------------------------------|-----------------------------------------------------|----------------------------|
| <b>1. Girdi</b>                                                         | <b>2. Yerel CLI</b>                                         | <b>3. Docker</b>                             | <b>4. Üç dosya</b>                               | <b>5. Tarayıcı</b>                                  | <b>6. İnsan</b>            |
| Bir baseline, bir candidate ve bir ile üç arasında temizlenmiş fixture. | Dosyaları sınırlı okur ve desteklenen kapsamı kontrol eder. | Her sürüm için ayrı, dışa kapalı n8n ortamı. | summary.json, report.md, evidence-manifest.json. | SHA-256 bağları sitede, yükleme olmadan doğrulanır. | Sürüm kararını kişi verir. |

## İş akışı değişikliğini dış sisteme dokunmadan prova et

Bu deneysel açık laboratuvardaki yerel komut satırı aracı, desteklenen başlangıç ve aday iş akışlarını ayrı Docker ortamlarında sentetik test verileriyle çalıştırır. HTTP eylemleri yalnız yerel yakalama servisine gider. Bu ekran oluşan üç dosyanın parmak izlerini tarayıcıda doğrular ve farkları okunabilir hale getirir.

### Ne kanıtlanır?

Gözlemlendi demek, dönüştürülmüş sentetik isteğin yerel yakalama servisine ulaştığı anlamına gelir. Düğüm çalışma sırası, insan onayları, yeniden deneme ve döngü davranışı, canlı sistem güvenliği veya penetrasyon testi sonucu kanıtlanmaz. Son sürüm kararı insandadır.

ai-agent-audit sayfasında Deneysel prova sekmesinin başı.

### Laboratuvar etiketi

Sayfa bu bölümü deneysel açık laboratuvar olarak işaretler. Ücretli teslim incelemesine dahil değildir.

### Ne kanıtlanır

Gözlendi kelimesinin tanımı sonucun üstünde durur. Böylece sınır, sonuçtan önce okunur. Ekran otomatik onay vermez.

## 3 Regresyon kapısı ve sekiz kontrolü

Kapı önce statik denetimi çalıştırır. Sonra sözleşmedeki testleri sırayla bir staging webhook'una gönderir. Her testte beklenen durum kodu ve JSON alanları kontrol edilir. Ayrı bir durum ucu, onaydan önce dışarıya hiçbir eylemin gitmediğini sayaçla doğrular.

**Kimlik doğrulama yok** Reddedilmeli.

**Geçersiz staging imzası** Reddedilmeli.

**Eksik ya da beklenmeyen alan** Reddedilmeli.

**Prompt injection işareti** Onay sınırının arkasında bekletilmeli.

**Geçersiz onay belirteci** Reddedilmeli.

**Geçerli istek** Dış eylem olmadan sıraya alınmalı.

**Tekrarlanan istek kimliği** Aynı işlemi döndürmeli.

**Desteklenmeyen metot** Reddedilmeli.

Hedef varsayılan olarak sadece yerel adres olabilir. Uzak bir staging için üç şey birden gerekir. Bunlar --allow-remote bayrağı, tam alan adı listesi ve dar yol önekleridir. Yönlendirmeler takip edilmez. Raporlar istek başlıklarını ve gövdelerini saklamaz.

Sitede daha önce kapının sentetik bir test workflow'u üzerindeki kayıtlı koşumu yeniden oynatılıyordu. Girdisi sentetik olduğu için 2 Ekim 2026'da yayından kaldırdım; kapıyı kendi staging ortamında çalıştırırsın.

## 4 Yerel sürüm provasının aşamaları

Prova node bin/rehearse.mjs komutuyla çalışır. Komuta baseline, candidate, fixture ve çıktı klasörü verilir. Docker Desktop açık olmalıdır.

|                                                                             |                                                                                           |                                                                                                        |                                                                                      |                                                                             |                                                                        |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------|
| <b>1. Sınırlı girdi</b><br>Bir baseline, bir candidate, bir ile üç fixture. | <b>2. Ön kontrol</b><br>Sadece desteklenen, credential kullanmayan workflow kabul edilir. | <b>3. Güvenli çevirme</b><br>Gerçek HTTP hedefleri kaldırılır, istekler yerel capture servisine gider. | <b>4. Ayrı ortam</b><br>Her sürüm için temiz n8n container ve volume. Dış ağ kapalı. | <b>5. Karşılaştırma</b><br>Planlanan eylem ile gözlenen eylem ayrı tutulur. | <b>6. Temizlik</b><br>Geçici kaynaklar silinir, sadece üç dosya kalır. |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------|

### Desteklenen kapsam bilerek dar

|                      |                                                                                                                                                     |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Giriş</b>         | Tek bir Webhook düğümü, sürüm 2.1, sabit POST yolu.                                                                                                 |
| <b>Ara adım</b>      | Sabit ve temizlenmiş değerli Set düğümleri, sürüm 3.4.                                                                                              |
| <b>Eylem</b>         | Credential kullanmayan HTTP Request düğümleri, sürüm 4.2, sabit POST, PUT ya da PATCH hedefi.                                                       |
| <b>Yapı</b>          | Döngüsüz tek bir main[0] yolu, en fazla 20 aktif düğüm.                                                                                             |
| <b>Durdurulanlar</b> | AI, Code, Execute Command, credential, alt workflow, topluluk düğümleri, dinamik hedefler, döngüler ve bilinmeyen sürümler Docker başlamadan durur. |

Sitedeki doğrulayıcı, provanın ürettiği üç dosyayı tarayıcıda açar. Sitede örnek bir prova paketi yayımlamıyorum, çünkü elimdeki paket sentetik fixture'lardan üretilmişti. Kendi provanın dosyalarını verdiğinde sonuç şu parçalarla açılır.

|                                   |                                                                                                                                            |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Sonuç</b>                      | Sonuç kodu ve altında üç dosyanın SHA-256 bağlarının eşleşip eşleşmediği. Eşleşme yalnızca paketin kendi içinde tutarlı olduğunu gösterir. |
| <b>Planlanan, gözlenen, eksik</b> | Üç sayı ayrı tutulur. Eksik sayısı sıfır değilse kanıt tamamlanmamıştır.                                                                   |
| <b>Gözlenen eylem farkı</b>       | Hangi düğümde neyin değiştiği, düz bir cümleyle.                                                                                           |
| <b>İzolasyon</b>                  | İzolasyon ve temizlik durumu, dış DNS sorgusu sayısı ve dışa iletim olup olmadığı.                                                         |

## 5 Sonuç kodları ve gözlendi kelimesi

|                               |                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------|
| <b>0, REHEARSAL_COMPLETE</b>  | Bütün desteklenen durumlar tamamlandı, beklenen kanıt gözlendi, eylem farkı yok. |
| <b>2, REVIEW_REQUIRED</b>     | Durumlar tamamlandı ve anlamlı bir eylem farkı var.                              |
| <b>3, BLOCKED_UNSUPPORTED</b> | Workflow desteklenen kapsamın dışında. Docker hiç başlamaz.                      |
| <b>4, INCOMPLETE_EVIDENCE</b> | Beklenen yakalama kanıtı eksik ya da çözülemedi.                                 |
| <b>5, CONTAINMENT_FAILURE</b> | DNS, dışa iletim, beklenmeyen eylem, envanter ya da temizlik kontrolü başarısız. |

Gözlendi, sadece dönüştürülmüş sentetik isteğin yerel capture servisine ulaştığı anlamına gelir. Düğüm çalışma sırasını, onay düğümünün gerçekten çalıştığını, yeniden deneme ve döngü davranışını, isteğin asıl hedefe ulaştığını, canlıya hazır olmayı ya da iki workflow'un bütünüyle eşdeğer olduğunu kanıtlamaz.

## 6 Tasarım kararları

- 1 Kapsamı dar tutmak**  
Desteklenmeyen bir şeyi tahminle çalıştırmak yerine durduruyorum. Bilinmeyen sürüm, dinamik hedef ya da credential görülürse sonuç BLOCKED olur.
- 2 Şüphede olumlu sonuç yok**  
Beklenmeyen bir DNS sorgusu, dışa iletim ya da temizlik hatası provayı başarısız sayar. Şüpheli varken olumlu sonuç yazılmaz.
- 3 İki sürüm asla aynı ortamda değil**  
Baseline ve candidate ayrı container ve volume kullanır. Dönüştürülmüş dosyalar orijinal SHA-256 değerlerine bağlı kalır.

**4****Sadece üç dosya yayımlanır**

Ham workflow, fixture gövdeleri, istek ve cevap içerikleri, başlık değerleri, credential ve Docker akışları çıktıya yazılmaz.

**5****Karar insanda**

Hiçbir çıktı sürümü onaylamaz. Site bile paketi doğruladıktan sonra kararı kişiye bırakır.

---

## 7 Sınırlar

- × Bu bir deneysel açık laboratuvarıdır. Sayfanın dediğı gibi ücretli teslim incelemesine dahil değildir ve ayrı bir runtime pilotu satılmaz.
- × Sonuç sadece verilen workflow'u, sözleşmeyi ve test senaryolarını kapsar. Penetrasyon testi, uyumluluk sertifikası ya da güvenlik garantisi değildir.
- × Prompt injection senaryosu bir dil modelini çağırır. Sadece onay çevresindeki workflow kontrollerini dener.
- × Genel kapı n8n'e yüklenen workflow'u geri okumaz. Staging'de gerçekten fingerprint'i alınan candidate'ın çalıştığını operatör ayrıca doğrulamalıdır.