

05

Kanıt kayıtları

1

Tümü 3

Yüksek 0

Orta 2

İncele 0

Bilgi 1

2

AS-203

Orta

Üçüncü taraf action tam commit SHA ile sabitlenmemiş

actions/checkout, değişebilir bir referans kullanıyor.

3

Konum

n8n-ai-agent-security-lab-main/.github/workflows/test.yml:18

4

Sıradaki insan kontrolü

Action'ı incelenmiş tam uzunlukta commit SHA ile sabitle ve okunabilir sürümü yorumda kaydet.

AS-203

Orta

Üçüncü taraf action tam commit SHA ile sabitlenmemiş

actions/setup-node, değişebilir bir referans kullanıyor.

Konum

n8n-ai-agent-security-lab-main/.github/workflows/test.yml:21

Sıradaki insan kontrolü

Action'ı incelenmiş tam uzunlukta commit SHA ile sabitle ve okunabilir sürümü yorumda kaydet.

AS-301

Bilgi

Bir ajan deposunda talimatları ve yetkileri bulmak

GitHub'dan indirdiğim bir depo arşivini tarayıcıda açıyorum. AI Agent Surface Map, ajana yön veren dosyaları, MCP bağlantılarını ve GitHub Actions izinlerini tek bir inceleme listesinde topluyor.

1 Bu araç ne işe yarar

Bir yapay zeka ajanının ne yapabileceği çoğu zaman kodda değil, küçük yapılandırma dosyalarında yazar. Bir talimat dosyası ajana kural verir. Bir MCP dosyası ona yeni bir araç bağlar. Bir GitHub Actions dosyası depoya yazma izni açabilir. Bunlar farklı klasörlere dağılır ve kolayca gözden kaçır.

Bu aracı, bir depoya tek kelimelik güvenli ya da güvensiz etiketi koymak yerine yetki veren parçaları tek tek görmek için yaptım. Araç arşivi sadece okur. Hiçbir dosyayı çalıştırmaz ve hiçbir sunucuya bağlanmaz.

1. Arşiv	2. Talimatlar	3. Araçlar	4. Dış eylem
GitHub'dan indirilen ZIP dosyası.	AGENTS.md, CLAUDE.md, skill ve Copilot dosyaları.	MCP sunucuları ve dosyada görünen komut, ağ, tarayıcı izleri.	GitHub Actions izinleri ve secret adları.

Birkaç kelime

Ajan	Kendi başına araç kullanabilen, dosya yazabilen ya da komut çalıştırabilen yapay zeka programı.
MCP	Model Context Protocol. Ajana dışarıdan araç bağlayan yapılandırma. Genelde .mcp.json gibi bir dosyada durur.
GitHub Actions	Depoda bir olay olduğunda kendiliğinden çalışan işler. Ayarları .github/workflows klasöründedir.
Secret	Parola ya da anahtar gibi gizli değer. Araç sadece adını görür, değerini rapora yazmaz.
Sabitleme	Bir paketi ya da Action'ı değişmeyecek tam bir sürüme bağlamak. Sabitlenmemiş parça yarın başka bir kod getirebilir.

2 Başlamadan önce

Gerekenler	İncelemek istediğin deponun ZIP dosyası. GitHub'da Code düğmesinden Download ZIP ile alınır.
Sınırlar	En fazla 12 MB ZIP, 1.200 arşiv kaydı, 320 desteklenen metin dosyası ve açılmış halde 16 MB veri. 512 KB'tan büyük tek dosyalar okunmaz.
Atlanan klasörler	.git, node_modules, vendor, dist, build, .next, coverage ve __pycache__.
Hesap	Gerekmez.
Veriler nerede	ZIP tarayıcıda açılır. Sunucuya gönderilmez. Kod ve MCP sunucuları çalıştırılmaz.

Büyük bir monorepo sınırı aşarsa araç durur ve nedenini yazar. O zaman sadece ilgilendiğin proje klasörünü ayrı bir ZIP olarak indir.

3 Arşivi açmak

Arşiv alanı. Sitede örnek arşiv yok; alan kendi ZIP dosyasını bekler.

1 Kendi ZIP dosyası seç

Dosya seçildiği anda tarayıcıda okunur. Birkaç saniye içinde aşağıdaki bölümler yeni arşive göre dolar.

2 Kanıt paketini indir

Tek bir ZIP iner. İçinde aynı sonucun JSON ve Markdown hali vardır.

3 Sınırı oku

Hangi boyuta kadar okunduğunu ve gizli değerlerin rapora eklenmediğini burada yazar.

4 Haritayı ve özeti okumak

Yüzey haritası, benim açık kaynak depom n8n-ai-agent-security-lab'ın GitHub ZIP'i ile. Kanıtın dosyadan inceleme notuna giden sırasını gösterir, kodun çalışırken ne yaptığını göstermez.

1

Repo arşivi

Arşivdeki kayıt sayısı.

2

Kalıcı talimatlar

Bulunan talimat dosyası sayısı. AGENTS.md, CLAUDE.md, GEMINI.md, copilot-instructions.md ve skills klasöründeki SKILL.md sayılır.

3

Araç ve bağlantılar

MCP sunucusu sayısı ile görünen yetenek türü sayısının toplamı.

4

Dış eylem yüzeyi

Okunan GitHub Actions dosyası sayısı.

03

İnceleme özeti

1

Yüksek

0

Orta

2

İncele

0

Bilgi

1

2

Okunan metin

123

MCP sunucusu

0

GitHub akışı

1

Talimat dosyası

1

İnceleme özeti. Önem kutularına basınca aşağıdaki liste o öneme göre süzülür.

1

Önem sayıları

Yüksek, Orta, İncele ve Bilgi. Kutuya basmak kayıt listesini o gruba indirir.

2

Ne okundu

Okunan metin dosyası, MCP sunucusu, GitHub akışı ve talimat dosyası sayıları. Beklediğin bir dosya sayılmadıysa arşivin içinde olup olmadığına bak.

Bir alt bölüm de *Görünen yetenekler* listesidir. Araç metin dosyalarında yerel komut, ağ erişimi, tarayıcı otomasyonu, dosya yazma, OSINT ve tehdit istihbaratı bağlayıcılarıyla ilgili belli kütüphane ve komut adlarını arar. Bir adın geçmesi, o yeteneğin gerçekten kullanıldığını göstermez.

5 Kanıt kayıtları

05

Kanıt kayıtları

1

Tümü 3

Yüksek 0

Orta 2

İncele 0

Bilgi 1

2

AS-203Orta

Üçüncü taraf action tam commit SHA ile sabitlenmemiş

actions/checkout, değişebilir bir referans kullanıyor.

3

Konum

n8n-ai-agent-security-lab-main/.github/workflows/test.yml:18

4

Sıradaki insan kontrolü

Action'ı incelenmiş tam uzunlukta commit SHA ile sabitle ve okunabilir sürümü yorumda kaydet.

AS-203Orta

Üçüncü taraf action tam commit SHA ile sabitlenmemiş

actions/setup-node, değişebilir bir referans kullanıyor.

Konum

n8n-ai-agent-security-lab-main/.github/workflows/test.yml:21

Sıradaki insan kontrolü

Action'ı incelenmiş tam uzunlukta commit SHA ile sabitle ve okunabilir sürümü yorumda kaydet.

AS-301Bilgi

Kanıt kayıtları. Her kayıt bir kural numarası, önem, konum ve bir sonraki insan kontrolünü taşır.

1 Süzgeç

Listeyi öneme göre daralt. Parantezdeki sayı o gruptaki kayıt sayısıdır.

2 Kural ve önem

AS ile başlayan numara hangi kuralın eşleştiğini söyler. Aynı numara JSON ve Markdown raporda da geçer.

3 Konum

Dosya yolu ve biliniyorsa satır numarası. Kararı vermeden önce bu dosyayı kendin aç.

4 Sıradaki insan kontrolü

Bu kayıt için bakman gereken şey. Araç bir düzeltme yapmaz, sadece nereye bakılacağını söyler.

Araç hangi durumlarda kayıt açar

AS-001	Arşivde .env benzeri bir ortam dosyası var. Yüksek. Değerleri okunmaz.
AS-100	MCP dosyası bulundu ama sunucu listesi çıkarılamadı. İncele.
AS-101	Bir MCP sunucusu yerel bir komut başlatıyor. Orta.
AS-102 / 103	Uzak bir MCP adresi var. HTTPS ise İncele, şifresiz HTTP ise Yüksek.
AS-104	MCP sunucusu ortam değişkeni adları istiyor. Orta.
AS-105	npx, uvx ya da pipx sürüm sabitlenmeden kullanılıyor. Orta.
AS-201	Actions dosyası pull_request_target tetikleyicisi kullanıyor. Yüksek.
AS-202	Actions dosyası write-all izni veriyor. Yüksek.
AS-203	Üçüncü taraf Action tam commit SHA ile sabitlenmemiş. Orta.
AS-204	Pull request ile çalışan iş secret kullanıyor. Orta.
AS-301	Depoda kalıcı ajan talimat dosyası var. Bilgi.

6 MCP kayıtları ve kanıt paketi

Arşivde MCP yapılandırması varsa her sunucu için dosya, taşıma türü ve komut ya da uzak adres listelenir. Ekran görüntüsü için kullandığım depoda MCP dosyası olmadığından bu kartları burada göstermiyorum.

Yerel sunucu	stdio taşıma, bilgisayarda bir komut başlatılacağı anlamına gelir. Ortam anahtarlarının sadece adı yazılır.
Uzak sunucu	remote taşıma, verinin başka bir adrese gideceği anlamına gelir. Araç bu adrese bağlanmaz. Sahibini ve neyi sakladığını ayrıca öğrenmen gerekir.

İşin sonunda kanıt paketini indiriyorum. ZIP içinde ai-agent-surface-report.json ve ai-agent-surface-report.md adlı iki dosya var. İkisi de özet sayıları, her kaydın kural numarasını, konumunu ve sınırları taşır. Gizli değerler iki dosyaya da yazılmaz.

7 Neyi yapmaz

- × Kodu, betikleri, Action paketlerini ve MCP sunucularını çalıştırmaz. Hiçbir uzak adrese bağlanmaz.
- × Bir kaydın çıkması istismar, zararlı yazılım ya da kötü proje kanıtı değildir. Kaydın çıkmaması da deponun güvenli olduğunu göstermez.

- × Dal koruması, depo ayarları, gerçek çalışma izinleri, bağımlılık uyarıları ve commit kaynağı arşivden görülemez.
- × Sadece desteklenen dosya adlarına ve metin kalıplarına bakar. Başka bir yerde tanımlanmış yetki gözden kaçabilir.

Arşivi saklamadan ya da biriyle paylaşmadan önce içindeki özel verileri temizle. Araç değerleri rapora yazmasa da ZIP dosyasının kendisi senin sorumluluğunda kalır.