

Üç gerçek n8n ajan değişikliği, teslimden önce incelendi

ReleaseGuard'ı herkese açık, MIT lisanslı bir n8n alert triage şablonundaki art arda üç değişiklik üzerinde çalıştırdım ve her sonucu tek tek okudum. Bu vaka araç çıktısını ve kendi notlarımı yan yana gösteriyor; aracın yanıldığı yerler de dahil.

Kaynak	https://github.com/scanner-inc/agents, n8n/alert-triage/workflow.json
İncelenen değişiklik	A: Ajana üç tehdit istihbaratı aracı ekleniyor B: İsteğe bağlı Jira kaydı oluşturma, kapalı olarak geliyor C: Ajan adım sınırı 10'dan 100'e çıkıyor
Motor	ReleaseGuard 1.3.0, 2026-09-30

Her sonucu okudum ve notları 30 Eylül 2026'da onayladım. Bu, herkese açık bir MIT şablonunun bağımsız incelemesi. Scanner'ın kendi sistemleri hakkında bir şey iddia etmiyor ve bir sızma testi değil.

1 Kaynak ve lisans

Workflow, herkese açık scanner-inc/agents deposundaki n8n/alert-triage/workflow.json dosyası. Bir webhook tespit alertini alıyor, bir yapay zeka ajanı okuma araçlarıyla inceliyor ve sonuç Slack'e yazılıyor. Dosyayı art arda gelen commitlerde karşılaştırdım. Workflow'u çalıştırmadım, hiçbir API'yi çağırmadım ve Scanner'ın hiçbir sistemine bakmadım. Bu yalnız herkese açık bir şablonun incelemesi; Scanner'ın kendi ürününü nasıl çalıştırdığı hakkında bir şey söylemiyor.

Workflow dosyaları Copyright (c) 2026 Scanner, Inc. olup MIT Lisansı ile yayımlanıyor. Bu inceleme bağımsızdır; Scanner ile bağlantılı değildir ve Scanner tarafından onaylanmamıştır. Ham workflow dosyaları burada yeniden yayımlanmıyor; aşağıdaki commit bağlantıları ve hashler tam sürümleri gösteriyor.

Her exportun sabitlenmiş verisinde bir örnek alert var; içinde bir tenant kimliği ve Scanner uygulamasına bir bağlantı bulunuyor. İkisini de bu sayfaya, kayıtlara ve rapora almadım.

Depoyu aç	https://github.com/scanner-inc/agents
MIT lisansını aç	https://github.com/scanner-inc/agents/blob/15a608933b52ae2acc43777d5a46d9e1fa795e92/LICENSE

Bu vakanın göstermedikleri

- Dışa aktarılan JSON'un statik bir karşılaştırması. Workflow'u, modeli veya sorgu API'lerinin hiçbirini çalıştırmadım.
- Scanner MCP sunucusunun hangi araçları sunduğunu göstermiyor. Export MCP istemcisini varsayılan araç seçimiyle bağliyor; ajan sunucunun açtığı her aracı alıyor.
- Canlı credential'lar, n8n instance ayarları ve alertleri gönderen taraf bana görünür değildi.
- Bu bir sızma testi, Scanner hakkında bir zafiyet hükmü, sertifika veya güvenlik garantisi değil.

2 Değişiklik A: Ajana üç tehdit istihbaratı aracı ekleniyor

Ne değişti

Alert Triage Agent'a üç HTTP aracı bağlanıyor. ThreatFox IOC Lookup, threatfox-api.abuse.ch adresine search_ioc sorgusu ve modelin doldurduğu bir IOC ile POST gönderiyor. OTX Pulse Search, otx.alienvault.com adresine modelin seçtiği bir anahtar kelimeyle GET gönderiyor. Feodo Tracker, Feodo Tracker IP engel listesini indiriyor ve girdi almıyor.

Sistem promptuna, ajana bu üç aracı ne zaman kullanacağını anlatan kısa bir bölüm ekleniyor. Webhook, Slack adımı ve model aynı kalıyor.

Önce	e425e65, 2026-04-23, "Rename Scanner bearer credential to Scanner API/MCP Bearer Auth account across all workflows" https://github.com/scanner-inc/agents/commit/e425e65c11cf64f5fc39e2f52027c490c66efe79
Sonra	03ccb47, 2026-04-23, "Add threat intel tools (ThreatFox, OTX, Feodo) to alert-triage and slack-bot" https://github.com/scanner-inc/agents/commit/03ccb47972ca8b364b3ed8698a7e825da134defb

Araç çıktısı

ReleaseGuard 1.3.0, yalnız dışa aktarılan JSON, staging çalıştırması yok.

Sonuç	İnsan doğrulaması tamamlandı. Sürüm kararı gerekli
Kayıtlar	0 engelleyici, 6 inceleme, 0 iyileştirme, 3 bağlam
Açık bulgular	1 bu değişiklikten, 6 önceden de vardı
Aynı çift, düzeltmelerden önce (motor 1.2.0)	Bu değişikliği durdur. Tek engelleyici TG-106 idi: ThreatFox sorgusu bir POST ve eski motor her POST'u yazma sayıyordu. (1 engelleyici, 5 inceleme, 0 iyileştirme, 3 bağlam)
CR-001, REVIEW	Yeni bir güvenlik bulgusu oluştu: AA-008
CR-002, REVIEW	Yeni bir dış hedef eklendi: feodotracker.abuse.ch
CR-003, REVIEW	Yeni bir dış hedef eklendi: otx.alienvault.com
CR-004, REVIEW	Yeni bir dış hedef eklendi: threatfox-api.abuse.ch
CR-005, REVIEW	POST isteği okuma amaçlı sorgu olarak değerlendirildi: ThreatFox IOC Lookup
CR-006, REVIEW	Güvenlikle ilgili yapılandırma değişti: Alert Triage Agent

İNCELEYEN NOTLARI, AHMET GÖKER, 30 EYLÜL 2026

Doğrulanalar

- CR-001, üç yeni araçta zaman aşımı veya yeniden deneme yok (AA-008). Yavaş veya erişilemeyen bir sorgu API'si ajan çalışmasını bekletir; ajan adımı da kendi başına 3 kez yeniden dener.

- CR-002 ile CR-004 arası, üç yeni dış hedef: ThreatFox ve Feodo Tracker için abuse.ch, bir de AlienVault OTX. Workflow'dan çıkan değer modelin seçtiği değer. ThreatFox için bu tek bir IOC. OTX Pulse Search için herhangi bir anahtar kelime; prompt IP, domain, CVE numarası, zararlı yazılım ve aktör adı öneriyor, ama modelin aleritten aldığı bir iç sunucu adını veya kullanıcı adını göndermesini engelleyen bir şey yok.
- CR-005, ThreatFox IOC Lookup yalnız okuma yapan bir sorgu. Gövde search_ioc istiyor; gövdede yazma anlamına gelen bir fiil olmadığını kontrol ettim.

Yanlış alarmlar

- Düzeltmeden önce ThreatFox'a giden POST yazma sayıldığı için TG-106 engelleyiciydi. İstek bir arama. Araç artık bunu engelleyici değil, incelenecek bir sorgu olarak kaydediyor.

Aracın kaçırdıkları

- OTX anahtar kelimesi URL sorgu metnine modelin yazdığı haliyle giriyor (q=...). Kodlama adımı yok; modelin metni URL'nin parçası oluyor. Host sabit kaldığı için etkisi düşük.
- Feodo Tracker, araç açıklamasında yazdığı gibi, her çağrıda engel listesinin tamamını modele veriyor. Bu her çalışmada bağlam ve maliyet demek. Listenin boyutunu ölçmedim.

Teslimden önce önerilen düzeltme

- Üç araçta yaklaşık 10 ile 15 saniyelik bir zaman aşımı ve tek bir yeniden deneme ayarlayın.
- OTX'i belirli bir gösterge türünün sorgusuyla sınırlayın. Bu dosyadaki bir sonraki commit (4abe04e, 24 Nisan 2026) bunu yaptı: OTX Pulse Search yerine OTX IOC Lookup koydu ve Feodo Tracker'ı kaldırdı.
- Teslim notuna abuse.ch ve AlienVault'a hangi değerlerin gittiğini yazın; müşteri bunun kabul edilebilir olup olmadığına karar verebilsin.

3 Değişiklik B: İsteğe bağlı Jira kaydı oluşturma, kapalı olarak geliyor

Ne değişti

Sistem promptu artık ajandan her cevabı ===JIRA=== işaretinden sonra bir Jira bloğuyla bitirmesini istiyor. Kaydın açılıp açılmayacağına model, promptta yazan bir kurala göre karar veriyor: SUSPICIOUS veya MALICIOUS sınıfı ve Medium ya da üstü alert önem derecesi.

Yeni bir Code adımı, Split Output, cevabı Slack metni ve Jira alanları olarak ikiye ayırıyor. Send a message artık bu Slack metnini gönderiyor. Yeni bir If adımı, Create Jira?, create_jira değerine bakıyor. Yeni bir Jira adımı, Create Jira Issue, modelin yazdığı başlık, açıklama, öncelik ve etiketlerle kayıt açıyor. Kapalı geliyor; commit mesajı workflow'un kutudan çıktığı haliyle yalnız Slack ile çalıştığını söylüyor.

Önce	cfcaea6, 2026-04-24, "Tighten alert-triage report formatting" https://github.com/scanner-inc/agents/commit/cfcaea60035aebf3cd9b2e324dc7d3a901f9b0ce
Sonra	15a6089, 2026-05-12, "Add optional Jira ticket creation to n8n alert-triage and threat-hunt" https://github.com/scanner-inc/agents/commit/15a608933b52ae2acc43777d5a46d9e1fa795e92

Araç çıktısı

ReleaseGuard 1.3.0, yalnız dışa aktarılan JSON, staging çalıştırması yok.

Sonuç	İnsan doğrulaması tamamlandı. Sürüm kararı gerekli
Kayıtlar	0 engelleyici, 3 inceleme, 0 iyileştirme, 5 bağlam
Açık bulgular	0 bu değişiklikten, 7 önceden de vardı
Aynı çift, düzeltmelerden önce (motor 1.2.0)	Bu değişikliği durdur. İki engelleyici, yeni diye raporlanan TG-100 ve AA-004 idi; aynı iki kural ayrıca çözüldü diye de raporlandı. Yalnız yollarındaki bir adım değişmişti. Kapalı Jira adımı yalnız bağlam olarak görünüyordu. (2 engelleyici, 2 inceleme, 2 iyileştirme, 3 bağlam)
CR-001, REVIEW	Kapalı gelen bir yazma yolu eklendi: Create Jira Issue
CR-002, REVIEW	Güvenlikle ilgili yapılandırma değişti: Alert Triage Agent
CR-003, REVIEW	Güvenlikle ilgili yapılandırma değişti: Send a message
CR-004, CONTEXT	Mevcut bir bulgu artık farklı adımları kapsıyor: TG-100
CR-005, CONTEXT	Mevcut bir bulgu artık farklı adımları kapsıyor: AA-004

Doğrulanalar

- CR-001, kapalı gelen ve model çıktısına göre karar veren bir kapının arkasındaki bir yazma yolu. Kaydın açılıp açılmayacağı ve içindeki her alan modelden geliyor. Split Output, Jira bloğunun JSON olarak okunduğunu ve create değerinin true olduğunu kontrol ediyor, olmazsa yalnız Slack'e düşüyor; bozuk çıktıya karşı gerçek bir koruma. Ancak sınıfı veya önem derecesini alertin kendisiyle karşılaştırmıyor. Jira adımını açmak editörde tek bir işlem.
- CR-003, Send a message değişti. Eski ifade siren emojisinden önceki her şeyi kesiyordu; yenisi Slack metnini olduğu gibi gönderiyor, yani modelin yazdığı her giriş cümlesi artık kanala gidiyor. Bakımcılar kesmeyi aynı gün a1dd1a6 commitinde geri koydu; bu da gerilemeyi doğruluyor.

Yanlış alarmlar

- Düzeltmeden önce TG-100 ve AA-004 hem yeni engelleyici hem de çözülmüş olarak raporlanıyordu. İkisi de hala webhook'ta başlayıp Send a message adımında bitiyor; araya yalnız Split Output eklendi. Araç artık her biri için tek bir bağlam satırı yazıyor.

Aracın kaçırdıkları

- Etiketler ve öncelik Jira'ya modelin yazdığı haliyle gidiyor. Jira bazı etiket karakterlerini reddediyor, bazı projeler de öncelik alanını kabul etmiyor. Bakımcılar ikisini de aynı gün a1dd1a6 commitinde düzeltti. Araç Jira'nın alan kurallarını bilemez.
- Kayıt sayısını sınırlayan bir şey yok. Bir alert yığını her alert için bir kayıt açabilir ve bir alertin yalnız tek kayıt açtığını kontrol eden bir adım yok.
- Önem derecesi eşiği workflow içinde bir kontrol değil, promptta bir cümle.

Teslimden önce önerilen düzeltme

- Create Jira Issue açılmadan önce: create_jira değerini Split Output içinde alertin kendi önem alanından (Webhook ögesinden okunarak) ve yalnız SUSPICIOUS veya MALICIOUS olabilen bir sınıftan hesaplayın.
- Etiketleri sabit bir listeyle sınırlayın, alert kimliğini tekrar kontrolü için anahtar yapın ve günlük bir kayıt üst sınırı koyun.
- Jira adımını açmayı ayrı bir değişiklik olarak ele alın ve ayrıca inceleyin.

4 Değişiklik C: Ajan adım sınırı 10'dan 100'e çıkıyor

Ne değişti

Tek bir alan değişiyor. Alert Triage Agent'a options.maxIterations değeri 100 olarak ekleniyor. Önceden alan yoktu, bu yüzden n8n'in varsayılan değeri olan 10 geçerliydi. Commit mesajı nedeni yazıyor: 10 ile ajanlar incelemenin ortasında duruyordu.

Önce	4abe04e, 2026-04-24, "Modernize n8n tool nodes and refactor OTX threat intel" https://github.com/scanner-inc/agents/commit/4abe04ef4057778425cd0200e657b7ac71db10f8
Sonra	9d6164e, 2026-04-24, "Bump n8n agent maxIterations to 100" https://github.com/scanner-inc/agents/commit/9d6164e147d540cbdfed1abdb43fac18a34c58df

Araç çıktısı

ReleaseGuard 1.3.0, yalnız dışa aktarılan JSON, staging çalıştırması yok.

Sonuç	İnsan doğrulaması tamamlandı. Sürüm kararı gerekli
Kayıtlar	0 engelleyici, 1 inceleme, 0 iyileştirme, 0 bağlam
Açık bulgular	0 bu değişiklikten, 7 önceden de vardı
Aynı çift, düzeltmelerden önce (motor 1.2.0)	Bu değişikliği durdur, ama değişikliğin kendisinde engelleyici yok. Tek kayıt genel bir yapılandırma değişikliği idi; durdurma kararı şablonda zaten olan bulgulardan geliyordu. (0 engelleyici, 1 inceleme, 0 iyileştirme, 0 bağlam)

CR-001, REVIEW Ajan sınırı gevşetildi: Alert Triage Agent

İNCELEYEN NOTLARI, AHMET GÖKER, 30 EYLÜL 2026

Doğrulanalar

- CR-001, ajan sınırı 10'dan (n8n varsayılanı) 100'e gevşetildi. Committeki gerekçe yerinde. Getirdiği şey: tek bir alert artık 100 ajan adımına kadar yol açabilir; her adım bir model çağrısı ve çoğu zaman bir araç çağrısı. Ajan adımı hata alınca 5 saniye arrayla 3 kez yeniden deniyor, yani alert başına en kötü durum yaklaşık 300 adım. Workflow ayarlarında çalışma zaman aşımı yok ve ajandan önce bir hız sınırı yok (AA-006, zaten vardı).

Yanlış alarmlar

- Yeni çıktıda yok. Düzeltmeden önce, riski maliyet ve çalışma süresi olan tek alanlık bir değişiklik için sonuç Bu değişikliği durdur idi; çünkü sonucu şablonda zaten olan bulgular belirliyordu.

Aracın kaçırdıkları

- Araç yeni sınırı raporluyor, ama bunu ajanın yeniden deneme sayısı ile çarpıyor ve workflow ayarlarında çalışma zaman aşımı olup olmadığına bakmıyor. İkisini elle ekledim.

Teslimden önce önerilen düzeltme

- İncelemeler gerektiriyorsa 100 kalsın, ama etrafına bir sınır ekleyin: workflow ayarlarında bir çalışma zaman aşımı, ajan adımımda en fazla bir yeniden deneme ve ajandan önce alertler için bir üst sınır veya tekrar kontrolü.
- Değişiklikten sonraki ilk hafta çalışma başına model harcamasını izleyin.

5 Şablonda zaten olan bulgular

Bu açık bulgular her değişiklikten önceki sürümde zaten vardı. AA-008, değişiklik A ile geldiği için B'den itibaren önceden var sayılıyor. Her kayıta listeleniyorlar, ama üç değişikliğin hiçbirinin kararını belirlemiyorlar.

İNCELEYEN NOTLARI, AHMET GÖKER, 30 EYLÜL 2026

CRITICAL TG-100	A prompt-injection source can steer a privileged action through the AI agent Webhook'tan Alert Triage Agent üzerinden Send a message adımına giden yol gerçek: alert JSON'unun tamamı prompta giriyor ve alert alanları saldırganın kontrol ettiği bir metin taşıyabilir, örneğin bir kullanıcı veya kaynak adı. Webhook header doğrulaması kullanıyor ve son adım tek bir sabit Slack kanalına yazıyor; en kötü sonuç yanlış veya yanıltıcı bir triage notu. Bu şablon için kritik değil, orta seviye derim.
HIGH AA-003	Untrusted input can reach a model without a visible validation boundary Doğrulandı. Prompt, istek ögesinin tamamı JSON.stringify ile yazılarak kuruluyor; öncesinde boyutu sınırlayan veya serbest metni ayıklayan bir adım yok. Bir triage ajanı için bu tasarım gereği; bu yüzden çağırabildiği araçların yalnız okuma yapması önemli.
HIGH AA-004	A model can reach an external write action without an approval step Doğrulandı ve tasarım gereği: model çıktısı onay adımı olmadan Slack'e gönderiliyor. Triage notunu kanala yazmak workflow'un amacı. Burada onay gerekmiyor, ama başka bir yere yazan her adımdan önce gerekiyor.
HIGH AA-006	No rate or cost boundary was detected before model usage Exportta görünür bir hız veya maliyet sınırı yok. Alertler header doğrulamasının arkasındaki tespit platformundan geliyor; sınır gönderen tarafta olabilir, export bunu gösteremez. Alert hızının nerede sınırlandığını ekibe sorun.
MEDIUM AA-005	No structured model-output validation was detected Doğrulandı. Slack metni, yalnız ilk siren emojisinden itibaren kesilen model çıktısı. Üzerinde şema kontrolü çalışmıyor.
MEDIUM AA-008	Outbound requests do not show an explicit timeout or retry policy Doğrulandı. HTTP araçlarında zaman aşımı ve yeniden deneme yok; yavaş bir sorgu API'si ajanın tüm çalışmasını bekletir.
LOW AA-010	No workflow-level failure route was detected Doğrulandı, düşük. Hata workflow'u tanımlı değil; başarısız bir triage çalışması, biri çalışma listesine bakmadıkça fark edilmez.