



Her alarmı inceleyen ve aksiyon alan yapay zekalı SOC analisti.

Ornis Guard; tehdit tespiti ve olay yönetimi için kurum içi çalışan bir yapay zekalı SOC analistidir. Farklı siber güvenlik teknolojilerinden gelen alarmları 7/24 triyaj eder, her kararını açıklar ve tehditleri kontrol altına alır.



AI

Alarm yoğunluğundan açıklanabilir kararlara

Güvenlik ekipleri her gün yüzlerce alarmı değerlendirmek zorunda. Çoğu yanlış pozitif; ancak her biri analist zamanı tüketir ve gerçek tehditlerin ortamda kalma süresini (dwell time) uzatır. Ornis Guard ham alarm kayıtlarını açıklanabilir, denetlenebilir ve aksiyona hazır güvenlik vakalarına dönüştürür.

SOC ve MDR ekipleri zamanı nerede kaybediyor?

- **Alarm yorgunluğu:**
Yüksek hacim ve tekrarlayan yanlış pozitifler gerçek tehditleri kuyruğun gerisine iter.
- **Manuel zenginleştirme:**
Tehdit istihbaratı, varlık ve kullanıcı bağlamı alarm elle toplanır.
- **Tutarsız triyaj:**
Kalite, o an kimin vardiyada olduğuna ve ne kadar zamanı olduğuna bağlıdır.
- **Yavaş devir:**
İnceleme ile müdahale arasındaki boşluk, saldırganın alan kazandığı yerdir.

Ornis Guard ile ne değişir?

- **Tam kapsam:**
Her alarm, uzmanlaşmış AI rolleri tarafından 7/24 triyaj edilir ve incelenir.
- **Tutarlı kararlar:**
Her vaka güven skoru, kanıt zinciri ve gerekçe taşır.
- **Daha hızlı müdahale:**
Politika tabanlı kontrol altına alma MTTD ve MTTR'yi birlikte kısaltır.
- **Birikimli bilgi:**
Analist ve müşteri geri bildirimleri kurumsal hafızaya dönüşür.

TDIR iş akışı — her alarm için altı adım

Her aşama uzmanlaşmış bir AI rolü tarafından yürütülür ve vaka zaman çizelgesine kaydedilir.

1. Topla

✓ ok

Yeni alarmları alır, filtreler ve tekrarları eler.

2. Zenginleştir

✓ 2.0s

IOC'leri tehdit istihbaratı, varlıklar ve kurumsal bağlamla ilişkilendirir.

3. İncele

✓ ok

Alarmı uzmanlaşmış AI rolleriyle adım adım değerlendirir.

4. Doğrula

✓ ok

Bağımsız kalite katmanı, sonucu sistemden çıkmadan önce denetler.

5. Müdahale et

● onay

Kararı ticket, e-posta veya Telegram ile iletir; kontrol altına almayı uygulamaya sunar; alarmı kaynağa kapatır.

6. Öğren

✓ ok

Analist ve müşteri geri bildirimlerini kurumsal hafızaya ekler.

Kapsam

Her Alarm

Trijaj edilir ve incelenir.
Örnekleme yok, kuyruk yok.

Açıklanabilirlik

Her Karar

Güven skoru, kanıt zinciri,
MITRE ATT&CK eşlemesi.

Müdahale

Her Aksiyon

Politika kapılı, loglanır, platform
izin verdiğinde geri alınabilir.

SOC ve MDR operasyonları için tek iş akışı:

Ornis Guard alarm özetlerinin ötesinde analiz, tehdit avı, kalite kontrol, vaka yönetimi, müşteri iletişimi ve kurumsal öğrenmeyi tek ve denetlenebilir bir iş akışında birleştirir.

Her alarm için açıklanabilir bir karar

Her alarm, uzmanlaşmış AI rolleri tarafından yürütülen beş aşamadan geçer. İnceleme sürecini canlı izleyin; kararın nasıl üretildiğini ve sistemin her adımda ne kadar emin olduğunu görün.

Web Attack: PHP-CGI Remote Code Execution Attempt (CVE-2024-4577)

Ornis Guard ID: 06-1140191 Alarm ID: 309682

IsNet

Yüksek (8/10)

Analiz edildi

Özet **Analizler** Zaman çizelgesi Analist notları İncele

Hunter Report Reviewer

TAMAMLANDI

24 Ağu, 15:55

• Gerçek tehdit

güven 0.94

✓ Dosya oluşturma izleri
bulgu yok

✓ Kalıcılık kontrolü
bulgu yok

✓ Yanal hareket taraması
bulgu yok

✓ C2 iletişim analizi
203.0.113.47 izleniyor



✓ Kalıcılık tespit edilmedi — etki kontrol altında, kanıtlar eklendi.

Beş aşama, beş uzmanlaşmış AI rolü

- 1 İlk değerlendirme** · Triyaj analisti
Alarmı sınıflandırır ve önceliklendirir; etkilenen varlıkları ve kullanıcıları belirler.
- 2 İnceleme planı** · İnceleyici
Gereken kanıtları ve çalıştırılacak sorguları belirler.
- 3 Tehdit avı** · Tehdit avcısı
İzin verilen kapsam içinde SIEM ve bağlı platformlarda kontrollü sorgular çalıştırır.
- 4 Kalite incelemesi** · Kalite denetçisi
Bağımsız QA rolü kanıtları, akıl yürütmeyi ve güven skorunu doğrular.
- 5 Karar ve aksiyon** · Müdahaleci
Gerekçeli kararı ilgili kanallara iletir ve vakayı müdahale politikasına devreder.

Analiz Çıktıları

- Karar**
Gerçek tehdit mi, yanlış pozitif mi?
- Güven ve önem derecesi**
Önceliklendirme için güven skoru ve önem seviyesi.
- Gerekçe**
Kararı destekleyen kanıt zinciri.
- Saldırı göstergeleri**
Çıkarılan IOC ve IOA verileri.
- Çerçeve eşlemesi**
MITRE ATT&CK teknikleri ve Cyber Kill Chain aşaması.
- Önerilen aksiyon**
Sınıflandırma, öncelik ve bir sonraki müdahale adımı.

Her rolün akıl yürütmesi vaka zaman çizelgesine kaydedilir. Analistler, denetçiler ve müşteriler aynı kanıt zincirini görür; hiçbir şey kara kutu değildir.

SIEM'in ötesinde: EDR, XDR ve NDR genelinde tespit ve müdahale

Ornis Guard yalnızca SIEM alarmlarıyla sınırlı değildir. Uç nokta, genişletilmiş ve ağ tespit platformlarından gelen tespitleri ve telemetriyi alır. Vakada ilişkilendirir ve MDR operasyonunun tamamını tespit, inceleme ve aktif müdahale ile kurumlar veya müşteriler için üstlenebilir.

SIEM

Girdi: Alarmlar, offense kayıtları ve log sorguları.

Müdahale: Alarmları kaynağa notlandırır ve kapatır.

EDR

Girdi: Uç nokta tespitleri, process ve dosya telemetrisi.

Müdahale: Cihazı izole eder, process sonlandırır, dosyayı karantinaya alır.

XDR

Girdi: Alanlar arası ilişkilendirilmiş olaylar.

Müdahale: Uç nokta, kimlik ve bulut sensörleri arasında aksiyonları koordine eder.

NDR

Girdi: Ağ tespitleri, yanal hareket ve C2 göstergeleri.

Müdahale: IP ve domainleri çevre güvenliğinde bloklar.

e-Posta güvenliği

Girdi: phishing ve zararlı yazılım tespitleri.

Müdahale: iletileri karantinaya alır, göndericileri bloklar.

Güvenlik duvarı / NGFW

Girdi: bağlantı ve politika olayları.

Müdahale: IP ve domain blok kurallarını iletir.

MDR Hizmeti için tasarlandı.

Çok kiracılı kurum ve domain yapısı · Müşteriye özel politikalar, istisnalar ve bilgi tabanı · Ticket ve e-posta ile müşteri iletişimi · Vardiya analizi ve yönetici raporları · SLA'ya duyarlı eskalasyon ve zaman aşımaları

Hibrit Müdahale Modu

Tespit ile aksiyon arasında bir karar motoru

Her karar, politika tabanlı bir karar motorundan geçer. Motor; güven skorunu, önem derecesini, varlık kritikliğini ve önerilen aksiyonun geri alınabilirliğini değerlendirir, ardından vakayı üç şeritten birine yönlendirir.

Güven skoru

Önem derecesi

Varlık kritikliği

Geri alınabilirlik

Kurum politikası

→

KARAR

ŞERİT 1 · OTONOM

Düşük riskli, geri alınabilir aksiyonlar anında uygulanır.

- Bilinen zararlı IP veya domaini blokla
- Phishing e-postasını karantinaya al
- Ticket aç, zenginleştir ve kapat

ŞERİT 2 · ONAY GEREKTİREN

Yüksek etkili aksiyonlar tek tıkla analist onayı bekler.

- Uç noktayı izole et
- Process sonlandır, dosyayı karantinaya al
- Müşteriye eskale et

ŞERİT 3 · YALNIZCA ÖNERİ

Düşük güven veya politika dışı: karar analistin.

- Belirsiz ya da çelişkili kanıt
- Kritik üretim varlıkları
- Playbook kapsamında olmayan aksiyonlar

• Onay gerekiyor

UZAK AKSİYON

Uç nokta izolasyonu

10.34.18.22 (FILESRV-02) EDR entegrasyonu üzerinden ağdan izole edilecek. Aktif oturumlar korunur; geri alma mümkündür.

Talep eden: Ornis Guard · Kapsam: tek uç nokta · Denetim: açık

İptal

Onayla

HER AKSİYONDA KORUYUCU SINIRLAR

- Kurum ve domain kapsamıyla sınırlı
- Aktör, gerekçe ve kanıtlarla loglanır
- Platform destekliyse geri alınabilir
- Zaman sınırlı, otomatik yeniden deneme
- Kaynak sisteme geri teyit edilir

Şüpheden kanıta otomatik inceleme

Tehdit avı

Av sorgularını AI ile üretin; başlatın, izleyin, tamamlayın ve kayıt altına alın.

```
index=auth user="mark.loward" earliest=-24h
| stats count by action
```

- SIEM'e özgü sorgu dili ve davranışı
- Kurum ve domain tabanlı yetki kapsamı
- Yalnızca izin verilen log kaynaklarında arama
- Başlatma, izleme, sonuç alma ve iptal
- Kalıcı sorgu ve sonuç geçmişi

Tehdit istihbaratı

Alarmlardan IP, domain, URL ve hash göstergelerini çıkarır; sağlayıcı sonuçlarını kurumsal bağlamla birleştirir.

203.0.113.47 · risk 92

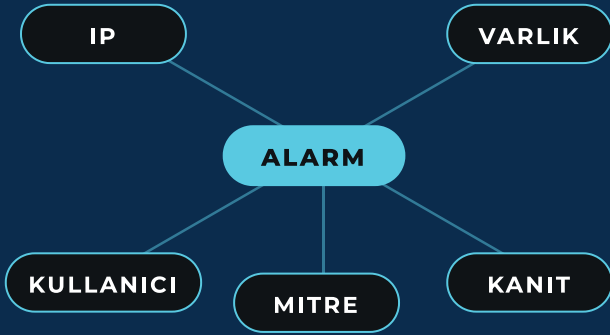
cdn-update.example · risk 61

sha256 9f3a...c2 · temiz

- Global ve kuruma özel API anahtar havuzları
- Sağlayıcı önceliklendirme ve sağlık izleme
- Normalize edilmiş risk skoru
- Kuruma özel istisna kuralları
- Varlık envanteri ve log kaynağı bağlamı

Tehdit haritası

Göstergeler, varlıklar, kullanıcılar, kanıtlar ve MITRE teknikleri tek bir ilişki görünümünde.



OG-1140002

Çözüldü

AI: TP

309680 – Exploit: Apache Struts RCE Payload Detected on DMZ Server [T1190]

- Ticket oluşturuldu
14:13:00 · Analiz iş akışı
- Bildirim e-postası gönderildi İletildi İletildi
14:13:25 · Analiz iş akışı
- SIEM alarmı kapatıldı · kaynak IP bloklandı
14:13:29 · Entegrasyon kuyruğu
- Çözüldü: bilinen olay
14:30:37 · Ornis Guard

İletişim ve Hafıza

Ticket ve müşteri geri bildirimi

Analizden otomatik ticket oluşturun. Durum geçişlerini, yorumları, olay geçmişini, dış aksiyonları, eskalasyonu ve zaman aşımını yönetin. Geri bildirimlerden otomatik bilgi kayıtları üretin.

Kurumsal bilgi tabanı (RAG)

Kayıtları kaynak türü, kalite, geçerlilik süresi ve alarm bağlamına göre yönetin. Her yeni vaka önceki deneyimden yararlanır.

VAKA → GERİ BİLDİRİM

→ KAYIT → HAFIZA ↻

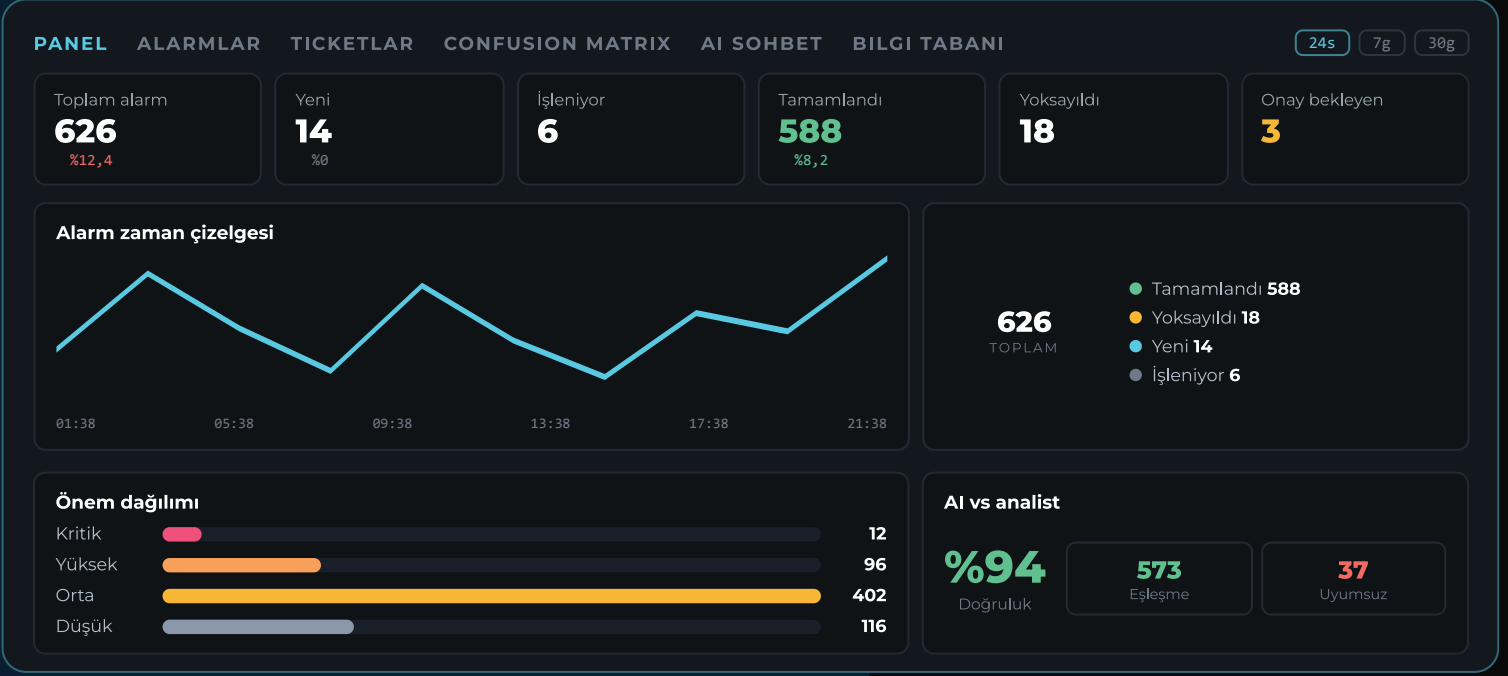
AI sohbet asistanı

Bunu L2 analiste eskale et.

L2 analizi tamamlandı: karar doğrulandı — Gerçek tehdit. Öneri: 10.34.18.22'yi izole et, 203.0.113.47'yi kara listeye al. 3.4 sn'de tamamlandı — insan devri gerekmedi

Tehdit istihbaratı, alarm analizi, varlık sorgusu, SIEM sorguları, IOC geçmişi, vardiya analizi — doğal dille.

SOC ve MDR operasyonlarını tek ekrandan yönetin



Temsili arayüz — gerçek müşteri verisi içermez. Gerçek zamanlı istatistikler · Durum ve zaman grafikleri · Vardiya analizi · Teknik ve yönetici raporları · TR / EN / NL arayüz

Alarm yönetimi

Arayın ve filtreleyin; tekil veya toplu incelemeleri başlatın ya da iptal edin. Alarmları yoksayın, sınıflandırın, eskale edin; bekleyen müdahale aksiyonlarını onaylayın.

Kanıt ve kalite

Zaman çizelgesini, kanıtları ve zenginleştirme verilerini görüntüleyin. Analist notlarını, etiketleri, kalite skorlarını ve güncellemeleri yönetin.

Raporlama ve denetim

CSV ve PDF çıktıları üretin. Doğruluğu confusion matrix ile izleyin; itirazları çözün; bildirimleri ve semantik arşivi yönetin.

Güvenlik ve Yönetim

Entegrasyon yönetimi

- API anahtarı veya kullanıcı bilgileriyle bağlantı
- Kurum ve domain tabanlı TLS doğrulaması
- Özel sertifikalar ve çok domainli teknoloji desteği
- Tarama aralığı ve alarm filtreleri
- Log kaynakları, varlık envanteri ve toplu içe aktarma

Güvenlik

- Veritabanında şifreli entegrasyon kimlik bilgileri
- Servisler arası ayrı kimlik doğrulama anahtarları
- Eksik yapılandırmada fail-secure davranış
- Yalnızca gerekli dış portlar
- Sıkılaştırılmış dağıtım ve güncel TLS

Denetim ve süreklilik

- Veri sınıfı ve kuruma göre saklama politikaları
- Tüm kullanıcı ve müdahale aksiyonları için denetim logları
- Sistem, sorgu ve tarama logları
- Başarısız dış aksiyonların otomatik yeniden denenmesi
- Her kritik işlem için izlenebilirlik



Verileriniz kurumunuzun içinde kalsın.

Ornis Guard, AI modelleri dahil tamamen kendi altyapınızda çalışır. Güvenlik verisi kurumdan hiç çıkmaz; her müdahale aksiyonu dahil tüm kritik işlemler izlenebilir ve denetlenebilir kalır.

Ornis Guard'ı kurumunuzun güvenlik operasyonlarında deneyimleyin.

Demo ve daha fazla bilgi için:

ornis.com.tr

info@ornis.com · 0850 290 0 290

