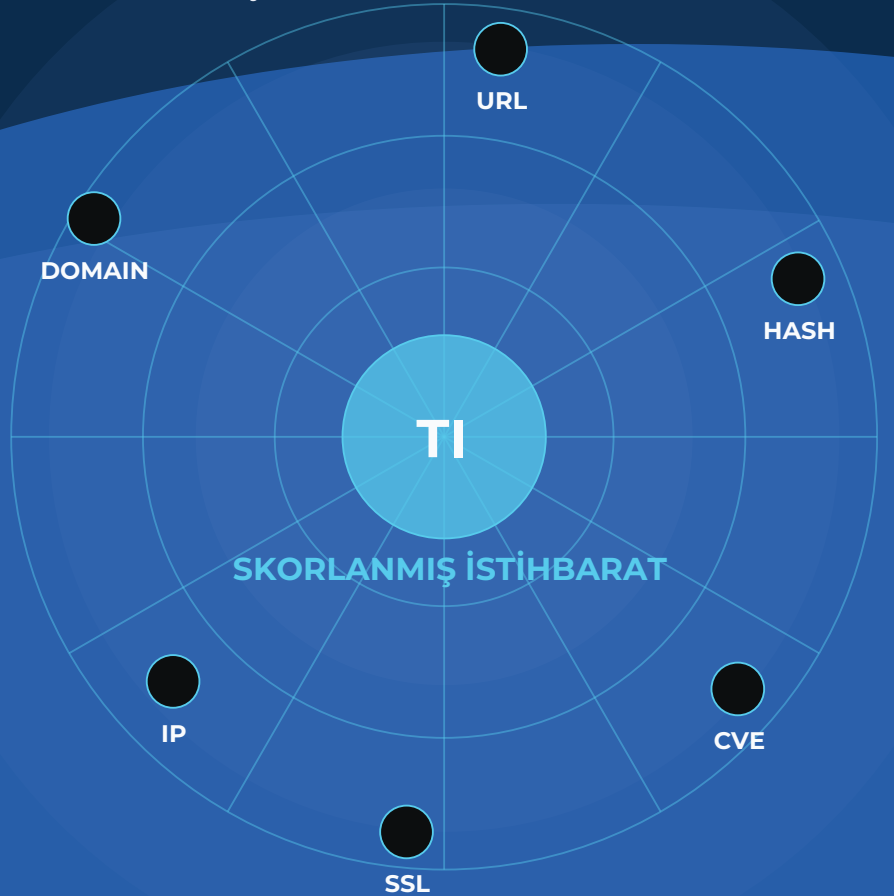




Dijital ayak izinizi saldırgandan önce görün.

Ornis Recon; internete açık varlıkları, ifşaları, sızmış kimlik bilgilerini, zafiyetleri ve tehdit göstergelerini skorlanmış, aksiyona hazır istihbarata dönüştüren çok kiracılı bir CTI platformudur. Dış saldırı yüzeyi görünürlüğünü, IoC analizini, ilişki grafiğini, raporlamayı ve müşteriye özel istihbarat servisini tek çatı altında birleştirir.



Dışarıdan görünen riskten kuruma özel istihbarata

Kurumların internete açık varlıkları sürekli değişir. Ornis Recon, güvenlik ekiplerinin kendileriyle ilgili olan tehdidi bulmasını ve önceliklendirmesini kolaylaştırır.

Görünmeyen risk nerede oluşuyor?

- Unutulmuş alt alan adları ve internete açık servisler
- Süresi dolan sertifikalar ve güncelliğini yitiren teknolojiler
- Sızıntı kaynaklarına düşen kurumsal hesaplar
- Birden fazla araçta parçalanmış gösterge ve itibar verisi
- Her müşteri için ayrı ayrı hazırlanan manuel raporlar
- İstihbaratı güvenlik araçlarına taşımak için yazılan özel entegrasyonlar

ornis recon neyi değiştirir?

- Her kuruma yalnızca kendi dijital risk görünümünü sunar.
- Kaynak güveni, güncellik ve çapraz doğrulamayı açıklar.
- Bulguları varlık, kimlik bilgisi, teknoloji ve CVE ile ilişkilendirir.
- Kaynakta kapanan bulguları otomatik pasifleştirir. İncelemeyi tek tıkla paylaşılabılır rapora dönüştürür.

İstihbarat iş akışı - altı adımda güncel görünürlük

Her bulgu, kaynağından müşteri portalına kadar izlenebilir ve denetlenebilir bir akışta işlenir.

1. Keşfet

Varlıkları, teknolojileri ve sertifikaları sürekli izle.

2. Tespit et

İfşa, kimlik bilgisi, zafiyet ve alarmı kuruma özel bul.

3. Doğrula

Çoklu kaynak ve MISP verisiyle çapraz kontrol et.

4. Skorla

0-10 TI skoru, itibar, konum ve ASN ile zenginleştir.

5. İlişkilendir

Varlık, alarm, teknoloji, kimlik bilgisi ve CVE bağlarını göster.

6. Sun

İzole portal, rapor ve dışa aktarımla paylaş.

Kapsam

Her müşterinin kendi dijital ayak izi

Kurum ve yetki kapsamıyla izole edilir.

Açıklanabilirlik

Her skorun kaynağı

Güven, güncellik ve doğrulama görünürdür.

Güncellik

Her bulgunun yaşam döngüsü

Kaynakta kapanan kayıtlar otomatik pasifleştir.

Tehdit alarmları

- ✓ Kuruma özel alarm, detay ve ekler
- ✓ Kritiklik, durum, tarih ve etiket filtreleri
- ✓ Varlık/kimlik/gösterge bağlantıları
- ✓ Platforma ait alarm referansları
- ✓ Otomatik pasifleştirme ve yetkili geçmiş

Dış saldırı yüzeyi

- ✓ Alan adı, IP ve servis envanteri
- ✓ Teknoloji ve sürüm tespiti
- ✓ SSL/TLS sertifika geçerliliği
- ✓ Varlık-teknoloji-CVE eşleşmesi
- ✓ Kaldırılan varlığın otomatik pasifleştirilmesi

İfşa ve kimlik bilgileri

- ✓ Açık servis, yapılandırma hatası ve sızıntı
- ✓ Kurum hesaplarının maskeli görünümü
- ✓ Hesabın alarm ve varlıkla ilişkilendirilmesi
- ✓ Yetkili açma ve denetim kaydı
- ✓ Premium erişim kontrolü

Zafiyet istihbaratı

- ✓ Teknolojiyle eşleşen CVE ve ayrıntıları
- ✓ Etkilenen varlık ve teknoloji bağlantısı
- ✓ Filtrelenebilir zafiyet listeleri
- ✓ Excel dışa aktarma

Güncel ve denetlenebilir kayıt yaşam döngüsü

Kaynakta kapanan alarm ve kaldırılan varlık otomatik pasifleştir; geçmiş kayıtlar yetkiye bağlı korunur ve ekranlar güncel kalır.

Bir gösterge için tüm resmi tek ekranda görün

IP, alan adı, URL veya hash; Ornis Recon sonucu şeffaf bir formülle puanlar, zenginleştirir ve geçmişleriyle birlikte saklar.

IOC LOOKUP

203.0.113.47

IP ADRESİ

TEHDİT İSTİHBARATI SKORU

8,7 / 10

5 kaynaktan doğrulandı

Skor bileşenleri

Kaynak güveni %92

Güncellik %78

Çapraz doğrulama %84

Zenginleştirme

KONUM İstanbul, TR

ASN AS64500

İTİBAR Kötüye kullanım: %64

TESPİT 7/18 motor

Geçmiş skor

Analistin kararını destekleyen dört katman



Tam eşleşme araması

Yetkili tüm istihbarat kaynaklarında göstergeyi arar.



Yerel coğrafi veri

Konum ve ASN bilgisini dışarıya sorgu göndermeden üretir.



Dayanıklı sorgulama

Önbellek ve günlük istek bütçesi dış servis kotalarını korur.



Kayıt ve kota

Müşteri bazlı günlük/haftalık kotalar; her sorgu denetim kaydında.

Arama ve zenginleştirme yetenekleri

Arama ve skor

- ✓ IP, alan adı, URL ve hash için çoklu motor tespit skoru
- ✓ Yetkili tüm kaynaklarda tam eşleşme araması
- ✓ Kaynak bazında güven skoru ve açıklayıcı rozetler
- ✓ Kötüye kullanım güven skoru ve rapor sayısı
- ✓ Sonuçların geçmişleriyle birlikte kalıcı saklanması

Zenginleştirme ve dayanıklılık

- ✓ Skorum zaman içindeki değişimini izleme
- ✓ Kurum bazında sağlayıcı açma/kapatma
- ✓ Önbellek ve günlük istek bütçesiyle kota koruması
- ✓ Servis erişilemezse aramanın kesintisiz sürmesi
- ✓ Etkileşimli 3B dünya küresinde konum görünümü

Ornis Recon; dış saldırı yüzeyini, tehdit alarmlarını, sızdırılmış hesapları ve varlıklarla eşleşen zafiyetleri tek merkezde ilişkilendirir. Güncel ve filtrelenebilir kayıt yapısıyla risklerin doğru bağlamda değerlendirilmesini, önceliklendirilmesini ve müşteriye özel çıktılara dönüştürülmesini sağlar.

Varlıkları görün • İlişkileri analiz edin • Riskleri önceliklendirin • Aksiyonu hızlandırın

Dış saldırı yüzeyinden ilişki grafiğine

Ornis Recon, internete açık varlıkları yalnızca envanterlemez; teknoloji, sertifika, zafiyet, alarm ve sızmış kimlik bilgileriyle ilişkilendirir.

✓ Alan adı

Alt alan adları, kurum ilişkisi ve güncel envanter

✓ IP ve servis

Açık portlar ve dışarıdan görünen servisler

✓ Teknoloji

Ürün, bileşen ve sürüm tespiti

✓ Sertifika

SSL/TLS geçerlilik ve sona erme takibi

✓ Zafiyet

CVE ayrıntıları; etkilenen varlık ve teknoloji bağı

✓ İfşa

Maskeli hesabın ilgili varlık ve alarmla ilişkisi

İnceleme grafiği

Varlık, alarm, kimlik bilgisi, teknoloji ve CVE bağlarını tek görünümde izleyin.



İnceleme grafiği

- Herhangi bir düğümden ilişkili bulguya anında geçiş
- İncelemeyi kaydetme ve kaldığı yerden devam etme
- Kurum kapsamına göre anlık dashboard ve grafikler
- Global arama ve veri tipine özel filtreler
- Grafik ekran görüntüsü ve eklerle HTML/PDF rapor
- Filtrelenebilir listelerden Excel dışı aktarma Web tabanlı açık ve koyu tema

Çok kaynaklı istihbarat, tek veri modeli

Ornis Recon; kendi tespitlerini, açık kaynak MISP topluluk istihbaratını ve harici itibar servislerini tek platformda birleştirerek doğrular.

Recon tespitleri

Kurumun dış yüzeyi

MISP

Standart ve premium

İtibar servisleri

Çapraz doğrulama

Senkronizasyon

Zamanlanmış / manuel

Anlık ilerleme takibi, iptal ve devam ettirme; aynı göstergenin kaç kaynakta doğrulandığı skora yansır.

Her müşteriye yalnızca kendi istihbaratı

Ornis Recon, MSSP'ler ve çok birimli kurumlar için müşteri izolasyonunu portal, arama, kota, raporlama ve premium veri erişimi boyunca korur.

Çok kiracılı istihbarat mimarisi



İzole portal

- ✓ Varlık, alarm, sızmış hesap ve CVE görünümü
- ✓ Portal ile IoC aramada aynı izolasyon
- ✓ Başka müşterinin verisi hiçbir ekranda görünmez

Sözleşme ve kota

- ✓ Premium veri yalnızca sözleşmesi olan müşterilere
- ✓ Müşteriye özel günlük/haftalık IoC arama kotası

Holding görünümü

- ✓ İştirak ve iş birimleri ayrı görünür
- ✓ Merkez ekipte birleşik risk resmi

Geçmişin korunması

- ✓ Hizmet askıya alınsa da geçmiş korunur
- ✓ Kayıtlar silinmeden erişim sınırlandırılır

Markanıza uygun istihbarat

Sağlayıcı izleri yerine sizin hizmetiniz görünür; dönüşüm kuralları kimlik ve ilişki bütünlüğünü korur.

İçerik dönüşüm kuralları

- ✓ Toplanan metinlere kaydedilmeden önce bul-değiştir uygulama
- ✓ Tam kelime, regex ve diğer eşleşme türleri
- ✓ Eşleşen içeriği değiştirme veya silme
- ✓ Kimlik, ilişki ve tarih alanlarını otomatik koruma
- ✓ Sağlayıcı izlerini müşteriye görünen marka diliyle değiştirme

Sürümlü ve kontrollü uygulama

- ✓ Kural setlerini sürümleyerek yönetme
- ✓ Geçmiş veriye uygulamadan önce etki önizlemesi
- ✓ Geçmiş veriye uygulamayı izleme ve gerektiğinde iptal etme
- ✓ Müşteriye görünen içeriği marka diline uyarlama

Tehdit istihbaratını tek merkezden yönetin

Dashboard, arama, raporlama, müşteri yönetimi ve güvenlik kontrolleri aynı web tabanlı operasyon ekranında buluşur.

RECON OVERVIEW

VARLIK

2.481

ALARM

126

İFŞA

38

CVE

594



● Kritik	14
● Yüksek	37
● İzlenen	75

Alarm ve varlık yönetimi

Kritiklik, durum, tarih ve etiket filtreleri; global arama ve güncel kayıt yaşam döngüsü.

Raporlama ve paylaşım

İnceleme grafiğini eklerle HTML/PDF rapora; listeleri Excel çıktısına dönüştürün.

Kaynak ve senkronizasyon

Sağlayıcıları kurum bazında yönetin; zamanlanmış ya da manuel senkronizasyonu izleyin.

Güvenlik ve Veri Gizliliği

Sağlayıcı izleri yerine sizin hizmetiniz görünür; dönüşüm kuralları kimlik ve ilişki bütünlüğünü korur.

Kurum içinde çalışır

- ✓ Müşteri istihbaratı üçüncü taraf buluta çıkmaz
- ✓ Tamamen on-premise dağıtım

Kimlik ve erişim

- ✓ Zorunlu TOTP iki faktörlü doğrulama
- ✓ CAPTCHA ve IP bazlı brute-force koruması
- ✓ Her ekran ve işlem için rol/kurum kapsamlı yetki

Veri koruması

- ✓ Sızmış kimlik bilgileri ve sırlar veritabanında şifreli
- ✓ Kimlik bilgileri ekranda maskeli
- ✓ Yetkili açma işlemi denetim kaydında

Denetim ve protokoller

- ✓ Kullanıcı, IP ve sonuç bazlı erişim kaydı
- ✓ TLS 1.2/1.3, CSP, HSTS ve CSRF koruması



Müşterilerinize sunacağınız istihbarat portalını görün.

Ornis Recon ile kurumunuza ve müşterilerinize ait dış riskleri tek platformda izleyin, doğrulayın ve raporlayın. İzole portal deneyimini görmek için demo talep edin.

Ornis Recon'u kurumunuzun güvenlik operasyonlarında deneyimleyin.

Demo ve daha fazla bilgi için:

ornis.com.tr

info@ornis.com · 0850 290 0 290

