ornis vista

Zafiyetlerinizi yalnızca tespit etmeyin, uçtan uca yönetin.

Ornis Vista; farklı güvenlik ürünlerinden gelen zafiyet verilerini, sızma testi bulgularını ve elle girilen kayıtları tek merkezde toplar. Bulguları varlıklarla eşleştirir, doğru ekibe atar, SLA ile kapanışa kadar izler ve yönetime ölçülebilir raporlar sunar. Kurumunuzun kendi sunucusunda çalışır.

işnet

Türkiye İş Bankası kuruluşudur. | TÜRKİYE İŞ BANKASI

Uçtan Uca Akış

Dağınık bulgulardan tek ve izlenebilir sürece

Her bulgu aynı yaşam döngüsüne girer. Otomatik adımlar kayıt düzenleme yükünü azaltır; ekipler açıkları kapatmaya odaklanır.

1. İçeri al
Güvenlik ürünlerinden entegrasyon veya dosya aktarımıyla veri al; sızma testi bulgularını ve elle girişleri aynı sürece kat.

2. Eşleştir
IP, host adı, FQDN veya URL ile varlığa bağla; yoksa oluştur, parmak iziyle tekrarı önle.

3. Önceliklendir
CVSS, varlık riski, CISA KEV, EPSS ve analist işaretleriyle ortam bazlı risk üret.

4. Ata
Varlık ekibi ve sahibi ile kuralları kullan; iş emri yoksa otomatik aç.

5. Çöz ve takip et
Durum geçişleri, pano, yorum ve ekler; dört göz onaylı risk kabulü.

6. Ölç
SLA uyumu, açık gecikmiş ve geç kapatılan ayrımı; ekip için 1-5 puan.

7. Raporla
Dashboard, 16 hazır rapor, yönetici raporu ve zamanlanmış e-posta.

6	3	9	16	10	4	2
Dosya Formatı	Giriş Yöntemi	Bulgu Durumu	Hazır Rapor	Hazır Rol	Planlama	Dil TR/EN

Bulgu kaynakları ve eşleştirme

- ✓ Desteklenen kaynak ve formatlar: Nessus API/.nessus, OpenVAS XML, Qualys XML, CSV, Excel ve JSON.
- ✓ Sızma testi raporlarını ve manuel bulguları içe aktarma; Türkçe/İngilizce kolonları otomatik tanıma..
- ✓ CSV ve Excel için kolon eşleştirme önizlemesi; atlanan satırları gerekçesiyle raporlama.
- ✓ Her kaynağı renkli etiketle gösterme.
- ✓ IP, host adı, FQDN veya URL ile varlığa bağlama; envanterde olmayan sunucu ve web uygulamasını otomatik oluşturma.
- ✓ Varlık, eklenti kimliği, port, protokol ve CVE parmak iziyle aynı zafiyet için ikinci kayıt açmama.

Güvenli ve kontrollü içe aktarma

- ✓ Makrolu Office dosyalarını reddetme, XML raporlarını güvenli ayrıştırıcıyla okuma.
- ✓ Tek dosyada 100.000 satıra kadar veri kabul etme.
- ✓ Yanlış yüklenen dosyanın bulgularını önizleme ve onayla geri alma; mevcut bulgulara dokunmama.
- ✓ Kaynak dosyadaki tarama, host ve önem sayılarını platformla karşılaştırma.
- ✓ Aktarılmamış bulguları tek tek listeleme; atlanan veya hatalı satırları gerekçesiyle gösterme.

Bir Sahibi

Her bulgu bir ekibe, gerektiğinde kişiye bağlıdır. Ekip değişirse bulgular ve iş emirleri birlikte taşınır.

Bir Süresi

Önem derecesine göre kapatma süresi işler; yalnızca tanımlı durumlarda ve sınırlı süre durur.

Bir Geçmişi

Atama, durum, önem, yorum ve SLA değişiklikleri kimin ne zaman yaptığıyla kaydedilir.

Sahiplik — Süre — İzlenebilir geçmiş

Ornis Vista'da her bulgunun bir sahibi, bir süresi ve bir geçmişi vardır.

Operasyon Disiplini

Her bulgu için doğru öncelik, doğru sahip, net süre

Tarayıcı önem derecesi başlangıçtır. Ornis Vista varlığın önemi ve ortam koşullarıyla riski yeniden değerlendirir; her kararı gerekçesiyle saklar.

Önem derecesi ve ortam bazlı risk

- ✓ Kritik, Yüksek, Orta, Düşük ve Bilgi seviyeleri; bulgu ve varlık risk skoru her gece yenilenir.
- ✓ İnternete açıklık, uzaktan sömürülebilirlik, aktif exploit, CISA KEV, EPSS, hassas veri ve telafi edici kontrol etkisi.
- ✓ Ağırlık ve eşikleri yönetici belirler; tarayıcı yeniden sınıflandırdığında geçmiş, SLA ve risk güncellenir.

Tekrar önleme ve karar koruma

- ✓ Varlık, eklenti kimliği, port, protokol ve CVE ile üretilen parmak izi aynı zafiyeti tanır.
- ✓ Yeni taramada kayıt açılmaz; son görülme, görülme sayısı, tarayıcı çıktısı ve CVSS güncellenir.
- ✓ False Positive veya elle kapatılan bulgu yeniden açılmaz; gerekirse elle açılır ve SLA yeniden başlar.
- ✓ Tam senkronda artık raporlanmayan, üzerinde çalışılmamış açıklar yalnız yeniden taranan varlıklarda kapanabilir.

Tanımlı yaşam döngüsü

Açık | **Devam Ediyor** | **Beklemede (3.Taraf)** | **Risk Azaltıldı** | **Çözüldü**

Risk Kabul | **False Positive** | **Kapalı** | **Yeniden Açıldı**

Kapatma ve False Positive işlemlerinde gerekçe zorunludur; kanıt dosyası eklenebilir. Bir iş emrine bağlı tüm bulgular kapandığında iş emri de kendiliğinden çözülür.

Atama ve yönlendirme

- ✓ Varlığın sorumlu ekibi ve sahibi; sızma testi dosyasındaki kişi ve ekiplerle otomatik atama.
- ✓ Önem, varlık türü/etiketi, kaynak ürüne özgü kontrol kimliği/ailesi ve CVE ile öncelik sıralı kurallar.
- ✓ Kritik/yüksek bulguyu ekip liderine, diğerlerini iş yükü en düşük üyeye verme; kaydetmeden örnekle test.
- ✓ Kendi ekibi, diğer ekipler veya tüm kurum için kademeli yetki; “Bu bizde değil” ile gerekçeli yönlendirme ve hedef ekibe bildirim.

SLA politikası ve bildirimler

- ✓ Kritik, Yüksek, Orta ve Düşük için kurumun belirlediği gün bazlı süreler; süre değişince yalnız etkilenen açık bulgu ve bağlı iş emirleri yeniden hesaplanır.
- ✓ Devam Ediyor ve Beklemede (3. Taraf) durumunda kurallı, sınırlı duraklatma; üçüncü taraf beklemesinde gerekçe zorunludur, sınır aşılınca süre yeniden başlar.
- ✓ Süre dolduğunda saatlik işaretleme; ihlal anı ve gecikme süresini kalıcı saklama; 1-5 SLA skoru.
- ✓ Son günlerde uyarı, ihlalde acil bildirim; atanmamış bulguyu ekip liderine gönderme; kanal ve sessiz saat tercihi.

  Açık gecikmiş ile geç kapatılanı ayrı raporlama; uyum oranını kurum genelinde tek tanımla hesaplama. Bulgu başına e-posta seli yerine günlük tek özet; ekip puanı eşikleri kuruma göre ayarlanır.

Bulguyla senkron iş emirleri

- ✓ Açık, Devam Ediyor, Beklemede, Çözüldü ve Kapalı durumları; çözüm açıklaması ve kapatma nedeni zorunlu.
- ✓ Son tarihi bulgu SLA’sından alma; Beklemede süresini sona ekleme.

  Elle, toplu, varlık detayından veya otomatik açma; çözüm ve kapanışı bulgularla çift yönlü eşleme.
- ✓ İş Emirlerim, Grubuma Atanan, Oluşturduklarım ve Tümü; toplu durum/atama ve Excel çıktısı.
- ✓ Açık, devam eden, çözülen iş emirleri; SLA ihlali, ortalama çözüm ve haftalık trend görünümü.

Risk Kabul Onayı

Gerekçe, geçerlilik ve kanıtla açılan talebi yetkili yönetici onaylar; talep eden kendi talebini onaylayamaz. Toplu onay ve dışa aktarma.

Zaman Çizelgesi

Durum, atama, önem, yorum, ek ve SLA ihlali; eski yorumlar denetim kaydında.

Toplu İşlem, Filtre ve Çıktı

Önem, durum, CVSS, SLA, ekip, sorumlu, varlık/tür, kaynak, etiket ve tarih filtresi. Paylaşılan bağlantı aynı görünümü açar. Toplu işlem açıklaması her bulgunun geçmişine ayrı işlenir; yetki dışı kayıtlar atlanıp bildirilir. 22 kolonlu Excel/CSV/PDF ve formül enjeksiyonu koruması.

Varlık ve Planlama

Varlık, bulgu ve iş emri aynı operasyon zincirinde

Ornis Vista envanteri taramalardan besler; sahipliği bulgulara ve iş emirlerine taşır. Planlama ve sızma testi süreçleri aynı ekranda izlenir.

Envanter ve sahiplik

- ✓ Sunucu, iş istasyonu, ağ cihazı, veritabanı, web/mobil uygulama, bulut kaynağı, konteyner ve IoT cihazı.
- ✓ Kritiklik: Kritik/Yüksek/Orta/Düşük; durum: Aktif/Pasif/Bakımda/Devre dışı. Silinen varlığın geçmişini koruma.
- ✓ Windows, Linux, macOS, iOS ve Android ailesini otomatik belirleme; filtredekilere toplu tür atama, eski ve yeni değeriyle denetim kaydı.
- ✓ Sorumlu ekip ve sahibi tek tek/toplu atama; atanan kişiye bildirim. Ekip değişince açık bulgu ve iş emirlerini taşıma; yeni bulguda sahipliği devralma.

Varlık görünümü ve veri kapsamı

- ✓ Rol kapsamına göre tüm varlıklar veya yalnızca ekip varlıkları; kapsam dışına bağlantıyla erişimi engelleme.
- ✓ Sahiplik değişikliklerini bulgulara ve iş emirlerine yansıtma; yeni bulguların ekip ve sorumluyu varlıktan devralması.
- ✓ Bağlantı paylaşılsa bile kapsam dışı varlığa erişimi engelleme.
- ✓ Silinen varlığın bulgu, iş emri ve denetim geçmişini koruma.

Toplu içe/dışa aktarma

Excel, CSV veya JSON şablonu; IP/host adıyla güncelleme, boş hücre mevcut veriyi silmez. Ekip sütununu düzenleyip geri yükleyerek toplu atama.

Yetkilendirme kaydı

SSH, RDP ve VPN erişimi; yetkili, yönetici, yerel/domain kullanıcıları, servis hesapları; sudo, veritabanı ve yedekleme yetkileri. Her güncelleme denetimde.

Port analizi

Port, protokol ve servisten varlık görünümü; RDP, Telnet, SMB ve veritabanı portlarını yerleşik risk kataloğuyla sınıflandırma ve Excel çıktısı.

Varlık detay sayfası

Özet

Ağ, sistem, sahiplik, bulut, son tarama, CVE ve SLA

Bulgular

Önem/durum, CVSS, port ve ilk tespit

İş Emirleri

Kritik/yüksek için tek tık; SLA teslim tarihi

Denetim

Oluşturma, güncelleme, toplu işlem ve yetki

Planlama: dört görünüm, beş sekme

- ✓ Pano (Kanban), Liste, Takvim ve Zaman Çizelgesi; Tümü, Bana Atanan, Takımım, Gecikmiş ve Arşiv sekmeleri.
- ✓ Açık, Devam Ediyor, Beklemede ve Çözüldü sütunlarında sürükle-bırak; sütundan yeni görev açma.
- ✓ Tür, önem, ekip ve sorumlu filtreleri; bulgu ve iş emirlerini aynı panoda izleme.
- ✓ Yapılacaklar listesi, renkli etiket, dosya eki ve değişiklik geçmişi; kişiye atama.
- ✓ Ek başına 10 MB; çalıştırılabilir dosya türlerini güvenlik gereği engelleme.

Sızma testi: rapordan gerçek kapanışa

- ✓ Firma/müşteri, 10 test türü, proje, teknik/iş sorumlusu, tarih ve durum; otomatik proje etiketi.
- ✓ IP, IP bloğu, alan adı, URL, mobil uygulama ve API dahil 8 kapsam öğesi; ortam/kritiklik ve Excel/CSV önizlemeli aktarım.
- ✓ İlk test, retest, final ve müşteri raporları dahil 5 rapor türünü; XLSX/CSV ham bulguları projede arşivleme.
- ✓ Test turlarını tarih, durum ve notla zaman çizelgesinde planlama; açık/kapanan/yeniden açılan bulguları gösterme.
- ✓ Pentest panelinde müşteri/proje/tarih filtresi, önem/durum, aylık trend, proje ve ekip; PDF, Excel ve CSV çıktısı.

Görünürlük ve Denetim

Analistten üst yönetime herkes için doğru tablo

Gösterge paneli rol ve veri kapsamına uyar. Yönetim, ekip ve analist aynı verinin kendi sorumluluğuna düşen bölümünü görür.

Dashboard ve hazır raporlar

- ✓ Varlık/bulgu, açık, yeniden açılan, risk kabul, kapalı ve SLA ihlali kartları; karttan filtreli liste.
- ✓ Hangi kartın hangi rolde görüneceği rol yönetiminden belirlenir.
- ✓ SLA uyumu, MTTR, son 12 haftanın gelen/kapanan trendi, önem/durum, bulgu yaşı, riskli varlık, yaygın CVE, ekip performansı, entegrasyon ve atanmamış kayıt.
- ✓ 16 rapor: Yönetici Özeti, SLA Uyumluluk, Ekip Performansı, süreç/MTTR/yaşlanma/iş emri/kapanış/tarama/kullanım ile Trend ve Top 10.

Yönetici ve zamanlanmış raporlama

- ✓ Seçilen ay için logolu kapaklı, önceki ay karşılaştırmalı yönetici raporunu tek tıkla Word/PDF üretme: risk, zafiyet dağılımı, kritik/yüksek, trend, SLA, riskli varlık, ekip, kapanan/yeni bulgu.
- ✓ Günlük, haftalık, iki haftalık veya aylık PDF/Excel/CSV raporu; her ekibe ayrı e-posta.
- ✓ Aylık kritik/yüksek özet; ekip ve kişi SLA performansını ay başında dondurarak sonradan değişmeyen kayıt.
- ✓ Aktivite, bağlı kullanıcı, yeni bulgu ve logların canlı yenilenmesi; tekrarlanan başarısız girişte kaba kuvvet uyarısı.

Hazır rapor kataloğu

Yönetici	SLA	Ekip	Süreç	Trend/Top 10
Varlık, açık, SLA, skor ve dönem hareketi	Önem bazlı uyum; zamanında/ihlal dağılımı	Açık/kapanan, geç kapanan, SLA ve MTTR	Yaşlanma, iş emri, kapanış, tarama ve kullanım	Riskli varlık, CVE, acil SLA ve en eski açık

Kimlik, dizin ve yetkilendirme

- ✓ e-Posta/parola; parolaları Argon2 ile özetleme. Google/Microsoft Authenticator TOTP; uygulamada kurum adını gösterme.
- ✓ LDAP/Active Directory girişi ve ilk girişte otomatik hesap; organizasyon birimi, departman, ekip ve yönetici ilişkilerini aktarma.
- ✓ Devre dışı dizin hesabını pasife alma; objectGUID/entryUUID ile ad/e-posta değişse de geçmişi koruma.
- ✓ LDAP gruplarını rollerle eşleme; yöneticinin elle verdiği/kaldırdığı rolleri koruma.

10 hazır rol, kuruma özel rol; modül/işlem, menü/panel kartı ve kendi/ekip/tüm veri kapsamı. Yetki değişikliği yeniden giriş olmadan geçerli.

Uygulama güvenliği, denetim ve SIEM

- ✓ Parola: en az 8 karakter, büyük/küçük harf, rakam ve özel karakter; yaygın parolayı reddetme. 30 dakikalık sıfırlama, anahtarı özetleme.
- ✓ Parola sıfırlamayı e-posta ile yapma; 30 dakika geçerli anahtarı veritabanında özetlenmiş saklama.
- ✓ Hareketsiz oturumu 30 dakikada kapatma; çıkışta/parola değişiminde oturum anahtarını iptal etme. HSTS, X-Frame-Options ve Referrer-Policy; sertifika tanımlı kurulumda HTTP'den HTTPS'e yönlendirme, yalnızca TLS 1.2/1.3.
- ✓ TOTP sırlarını şifreleme. Giriş, başarısız deneme, parola/MFA, kullanıcı/rol, varlık, bulgu, iş emri, tarama ve rapor hareketlerini kim/zaman/IP ile kaydetme.
- ✓ Yetkisiz denemeyi eksik izin/adres/IP ile kaydetme; filtre, ayrıntı ve Excel. Varsayılan saklama 5 yıl, yapılandırılabilir.
- ✓ API oluşturma/güncelleme/silme işlemlerini kullanıcı, kaynak IP ve sonuçla; denetim ve web erişimini ayrı LEEF 2.0 dosyalarına yazma. Parola/tokenı maskeleme, istek gövdesini yazmama; ortak istek kimliği ve rsyslog ile QRadar/SIEM aktarımı.

Kimlikten SIEM'e denetim zinciri

Kimlik	Denetim	İz	Korelasyon	Aktarım
LDAP/AD, e-posta/parola, TOTP	Rol, işlem ve veri kapsamı	Kim, ne zaman, hangi IP ile	Ortak istek kimliği	Ayrı LEEF 2.0 dosyaları, rsyslog

Altyapı ve Kullanım

Kurum içinde çalışan, güvenli ve denetlenebilir mimari

Uygulama ve veritabanı kurumun Linux sunucusunda barınır. Güncellemeler internet bağlantısı gerektirmeden arayüzden yüklenir.

Kurum içi kurulum

- ✓ PostgreSQL, Redis ve Nginx ile sistem servisi; Docker gerekmez.
- ✓ Kurulum betiği kaynakları denetler; isteğe bağlı SSL, güvenlik duvarı, SSH, dosya izinleri ve fail2ban.
- ✓ SLA kontrolleri, rapor ve tarayıcı senkronları ek iş kuyruğu servisi olmadan uygulama içinde zamanlanır.

Şifreli, internetsiz güncelleme

- ✓ AES-256 şifreli sürüm paketini Sistem > Güncelleme sayfasından yükleme.
- ✓ Önce otomatik veritabanı yedeği; başarısız işlemde önceki sürüme dönüş.
- ✓ İlerleme, canlı log ve sürüm notlarını aynı ekranda izleme.

Kendi kendine bakım

- ✓ Her gece ve yeniden başlatmada kapanan servisleri açma, disk doluluğunu denetleme ve logları döndürme.
- ✓ Haftalık veritabanı yedeği.
- ✓ Uygulama, veritabanı ve Redis sağlık uç noktalarını kurumun izleme araçlarına bağlama.

Entegrasyonlar ve bildirimler

- ✓ Güvenlik ürünlerinden API veya desteklenen dosya formatlarıyla veri aktarımı; bulguları doğrulama ve varlıklarla eşleştirme.
- ✓ Kurum SMTP'si (TLS/SSL): zafiyet, iş emri, varlık, SLA, risk kabulü ve sistem olayları için kurumsal HTML şablonlar.
- ✓ Webhook: bulgu, iş emri, varlık ve tarama olaylarını Teams, Slack veya HTTP adresine HMAC-SHA256 imzalı gönderme.
- ✓ SIEM: LEEF 2.0 denetim ve web erişim loglarını rsyslog ile aktarma.

Kurumsal kimlik ve kullanım

- ✓ Beyaz etiket: ürün adı, şirket bilgileri, logo, sekme simgesi ve giriş ekranı; e-posta ve PDF'de aynı kimlik.
- ✓ Türkçe ve İngilizce arayüz; sayfa yenilemeden dil değişimi.
- ✓ Açık/koyu tema; tablet ve telefon ekranlarına uyum.
- ✓ Merkezi portal üzerinden etkinleştirme veya internetsiz kurulum için imzalı çevrimdışı lisans.

Kurulum

Linux · PostgreSQL · Redis · Nginx · Docker yok

Donanım

4 GB RAM · 20 GB disk · 2 çekirdek önerilir

Çıktılar

PDF · Excel · CSV · Word/PDF yönetici · LEEF 2.0

Ornis Vista kimlerin işini kolaylaştırır?

Kurumsal BT

Farklı güvenlik ürünlerinden gelen bulguları Excel yerine sahipliğe dayalı ve izlenebilir bir süreçte yönetir.

SOC ve Güvenlik

Tarama, sızma testi ve manuel bulguları ortak risk, SLA ve kapanış sürecinde birleştirir.

Sızma Testi/ Denetim

Sızma testi bulgularını proje, retest ve doğrulanmış kapanış sürecine taşır.

Yönetim ve Performans

On-premise denetim izi, aylık rapor ve dondurulan performans sunar.

ornis vista

Kendi verinizle deneyin.

Ornis Vista, lisans anahtarı girilmeden 30 günlük deneme modunda çalışır. Kurulum ve kavram kanıtlama (PoC) çalışması için İşNet ekibiyle iletişime geçin.

Ornis Vista'yı kurumunuzun güvenlik operasyonlarında deneyimleyin.

Demo ve daha fazla bilgi için:
ornis.com.tr
info@ornis.com · 0850 290 0 290