

Vectra NDR

Yapay Zekâ Destekli Hibrit Ağ ve Kimlik Güvenlik Platformu

Vectra NDR; ağ, kimlik ve bulut ortamlarındaki saldırgan davranışlarını analiz ederek çok sayıdaki güvenlik sinyali arasından gerçekten müdahale gerektiren tehditlerin öne çıkarılmasına yardımcı olur. AA Teknoloji, Vectra NDR'ı mevcut SOC, uç nokta ve ağ güvenliği çözümleriyle birlikte konumlandırarak POC yönetimi, yerinde kurulum, entegrasyon, lisans yönetimi, ürün eğitimi ve SLA kapsamında Türkçe teknik destek süreçlerini uçtan uca yürütür.

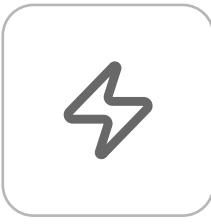
Modern Güvenlik Zorlukları

Hibrit yapılar da ağ trafiği, kimlik aktiviteleri, bulut servisleri ve yönetilmeyen varlıklar farklı güvenlik katmanlarında izlenir. Geçerli kimlik bilgilerini kullanan veya ağ içinde yanal hareket eden saldırganlar, tekil alarmlar arasında yeterli bağlam kurulamadığında gözden kaçabilir. Yüksek alarm hacmi de SOC ekibinin hangi olayın gerçekten öncelikli olduğunu belirlemesini zorlaştırır.

⚠ Hangi Ekiplere Hitap Eder?

- Şifrelenmiş trafik ve yanal hareketlerdeki tehditleri göremeyen SOC ekiplerine
- Kimlik suistimali ve ayrıcalık yükseltme girişimlerini izlemek isteyen kurumlara
- Yüksek alarm hacmi nedeniyle gerçek tehditleri önceliklendiremeyen ekiplere
- Hibrit ve çok bulutlu ortamlarda ağ ve kimlik davranışını birlikte değerlendirmek isteyen kurumlara

Temel İlkeler

			
Gözlemlenebilirlik	Hız	Kontrol	Sinyal
Ağ ve kimlik davranışını birlikte görme	Öncelikli tehdide daha hızlı odaklanma	Maruziyeti ve saldırı yayılımını azaltma	Gerçek saldırgan davranışlarını öne çıkarma

Vectra NDR Nasıl Çalışır?

Vectra NDR, ağ ve kimlik ortamlarından gelen davranışları birlikte değerlendirerek birbirinden kopuk sinyallerin aynı saldırının parçası olup olmadığını anlamaya yardımcı olur. Attack Signal Intelligence yaklaşımı, analistin çok sayıdaki alarm yerine öncelikli saldırı davranışlarına odaklanmasını sağlar.

Teknik Özellikler

📁 Gözlemlenebilirlik ve Kapsam

- ✓ Şirket içi, AWS, Azure, GCP ve Oracle Cloud desteği
- ✓ Microsoft 365, Active Directory ve Entra ID entegrasyonu
- ✓ IoT/OT, edge ve SaaS ortam desteği
- ✓ Agentless kurulum ve dakikalar içinde görünürlük

📁 Tespit Yetenekleri

- ✓ 200+ davranışsal tespit modeli
- ✓ 12 MITRE ATT&CK referans kategorisi
- ✓ Attack Signal Intelligence
- ✓ Şifrelenmiş trafikte deşifre gerektirmeme

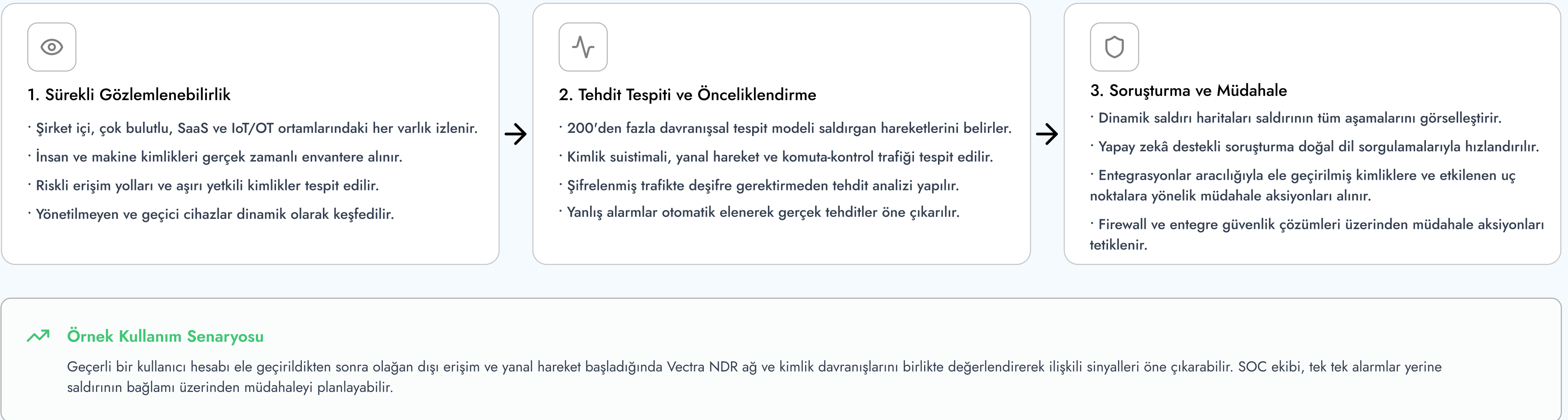
📁 Entegrasyonlar

- ✓ CrowdStrike Falcon, Microsoft Defender, SentinelOne
- ✓ Microsoft Sentinel, Splunk, Google SecOps
- ✓ Cortex XSOAR, Splunk SOAR
- ✓ Firewall, ITSM ve packet broker entegrasyonları

📁 Uyumluluk ve Raporlama

- ✓ NIST CSF 2.0, NIS2 ve Zero Trust uyumluluğu
- ✓ Uyumluluk denetimlerini destekleyen raporlama ve kanıt üretimi
- ✓ Üst yönetime yönelik güvenlik durum raporları
- ✓ MITRE ATT&CK framework uyumluluğu

Çalışma Akışı



Avantajlar

 Attack Signal Intelligence Dağınık sinyalleri saldırı bağlamında ilişkilendirerek analistin hangi tehdide önce bakması gerektiğini anlamasına yardımcı olur.	 Hızlı Soruşturma ve Müdahale Dinamik saldırı grafikleri ve yapay zekâ destekli soruşturma ile analistler tam saldırı hikâyesini kavrar; müdahale süresini önemli ölçüde kısaltır ve saldırıların yayılmasını engeller.
 Ağ ve Kimlik Görünürlüğü Şirket içi, çok bulutlu, SaaS, edge ve IoT/OT ortamlarındaki her varlık ve kimliği sürekli izler; statik envanter listelerinin aksine gerçek zamanlı aktiviteye dayalı dinamik bir saldırı yüzeyi görünümü sunar.	 Mevcut Güvenlik Ekosistemleri ile Entegre CrowdStrike ve Palo Alto Networks gibi çözümlerle birlikte tespit ve müdahale süreçlerini tamamlayabilir.