aa teknoloji

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 yapılarda 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
Ağ ve kimlik davranışını birlikte görme

Hız
Öncelikli tehdide daha hızlı odaklanma

Kontrol
Maruziyeti ve saldırı yayılımını azaltma

Sinyal
Gerçek saldırgan davranışlarını öne çıkarma

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

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.

Çalışma Akışı

1. Sürekli Gözlemlenebilirlik
- Şirket içi, çok bulutlu, SaaS ve IoT/OT ortamlarındaki her varlık izlenir.
- İnsan ve makine kimlikleri gerçek zamanlı envantere alınır.
- Riskli erişim yolları ve aşırı yetkili kimlikler tespit edilir.
- Yönetilmeyen ve geçici cihazlar dinamik olarak keşfedilir.

→

2. Tehdit Tespiti ve Önceliklendirme
- 200'den fazla davranışsal tespit modeli saldırgan hareketlerini belirler.
- Kimlik suistimali, yanal hareket ve komuta-kontrol trafiği tespit edilir.
- Şifrelenmiş trafikte deşifre gerektirmeden tehdit analizi yapılır.
- Yanlış alarmlar otomatik elenerek gerçek tehditler öne çıkarılır.

→

3. Soruşturma ve Müdahale
- Dinamik saldırı haritaları saldırının tüm aşamalarını görselleştirir.
- Yapay zekâ destekli soruşturma doğal dil sorgulamalarıyla hızlandırılır.
- Entegrasyonlar aracılığıyla ele geçirilmiş kimliklere ve etkilenen uç noktalara yönelik müdahale aksiyonları alınır.
- Firewall ve entegre güvenlik çözümleri üzerinden müdahale aksiyonları tetiklenir.

Örnek Kullanım Senaryosu

Geçerli bir kullanıcı hesabı ele geçirildikten sonra olağan dışı erişim ve yanal hareket başladığında Vectra NDR ağ ve kimlik davranışlarını birlikte değerlendirerek ilişkili sinyalleri öne çıkarabilir. SOC ekibi, tek tek alarmlar yerine saldırının bağlamı üzerinden müdahaleyi planlayabilir.

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.

aa teknoloji

AA Teknoloji, Anadolu Ajansı iştiraki olarak medya teknolojileri, siber güvenlik ve açık kaynak çözümleri alanlarında hizmet sunan bir teknoloji şirketidir. SOC hizmetleri, sızma testi, SIEM/EDR, tehdit istihbaratı ve medya altyapısı çözümlerini kurulum, entegrasyon ve 7/24 yerel teknik destekle birlikte sunar.

Daha fazla bilgi için, aateknoloji.tr'yi ziyaret edin veya @aateknoloji LinkedIn hesabını takip edin.