aa teknoloji

Sangfor Athena NDR

Ağ trafiğini gerçek zamanlı analiz eden, siber tehditleri ve anomalileri yapay zekâ ile tespit eden; gelişmiş görünürlük, tehdit avcılığı ve otomatik ağ koordinasyonu sağlayan ağ izleme ve müdahale platformudur.

Modern Ağ Güvenliği Zorlukları

Kurumsal ağların büyümesi, bulut entegrasyonları ve şifreli trafik hacminin artması, ağ genelinde kör noktalar oluşturmaktadır. Geleneksel güvenlik duvarları ve imza tabanlı sistemler, ağ içerisine sızmış ve gizlenen tehditleri tespit etmekte yetersiz kalmaktadır.
Saldırganların ağ içinde gerçekleştirdiği yanal hareketler (lateral movement), veri sızdırma girişimleri ve içerideki tehditler (insider threats) uzun süre fark edilmeden aktif kalabilir. Bu durum, kurumsal veri merkezleri ve kritik altyapılar için büyük risk oluşturur.
Farklı ağ segmentlerinden gelen devasa trafik verisinin manuel olarak analiz edilmesi ve anlamlandırılması imkansızdır. Güvenlik ekiplerinin bağlamsal analiz eksikliği, gerçek tehditler ile yanlış alarmları ayırt etmesini zorlaştırır.

⚠ Hangi Sorunları Çözer?

- Ağ trafiğindeki kör noktalarda gizlenen tehditlerin görünürlüğünün sağlanması.
- Ağ içindeki yanal hareketlerin (lateral movement) ve veri sızdırma girişimlerinin tespit edilmesi.
- Şifreli trafik (encrypted traffic) içindeki zararlı aktivitelerin analiz edilmesindeki zorlukların giderilmesi.
- Tehdit müdahale süreçlerinin otomatize edilmesi ve saldırı zincirinin (attack chain) uçtan uca izlenebilmesi.

Temel İlkeler

Derin Görünürlük
Ağdaki tüm kör noktaları ortadan kaldırarak tam kontrol sağlar.

Akıllı Analiz
Yapay zekâ ile şüpheli davranışları ve anomalileri tespit eder.

Hızlı Sınırlama
Saldırının ağ geneline yayılmasını anında otomatik engeller.

Bütünleşik Yanıt
Ağ ve uç nokta sistemlerini entegre bir savunmaya dönüştürür.

Sangfor Athena NDR Nasıl Çalışır?

Sangfor Athena NDR (Cyber Command), kurumsal ağ genelindeki ayna (mirror) trafik verilerini veya akış loglarını merkezi altyapısında toplayarak çalışır. Toplanan veriler yapay zekâ modelleri ve makine öğrenimi algoritmaları ile analiz edilerek ağ anomalileri belirlenir. Bir siber saldırı zinciri tespit edildiğinde sistem alarm üretir ve entegre güvenlik ürünleri aracılığıyla tehdidi otomatik olarak izole eder.

Teknik Özellikler

Ağ Trafiği Analizi (NTA)
- Gerçek zamanlı derin paket inceleme (DPI)
- Kuzey-Güney ve Doğu-Batı trafiği izleme
- Şifreli trafik analizi (ETA) desteği
- NetFlow, IPFIX ve ayna trafik toplama

Gelişmiş Tehdit Algılama
- Yapay zekâ tabanlı davranışsal anomali tespiti
- MITRE ATT&CK taksonomisi ile tam uyum
- Bilinmeyen tehdit ve sıfırıncı gün tespiti
- Komuta Kontrol (C2) merkezi iletişimi takibi

Saldırı Zinciri Görselleştirme
- Grafik tabanlı siber saldırı zinciri analizi
- Tehditlerin kök neden (root-cause) analizi
- Etkilenen varlıkların ve cihazların tespiti
- Adli bilişim (forensics) ve kayıt analizi

Güvenlik Orkestrasyonu ve Müdahale
- Güvenlik duvarları üzerinden otomatik IP engelleme
- EDR entegrasyonu ile uç nokta karantinası
- REST API üzerinden harici sistem uyumu
- Esnek ve otomatik müdahale playbook yapısı

Danışmanlık ve Yönetilen Hizmetler
- Ağ topolojisi analizi, trafik hacmi ölçümü ve donanım/sensör konumlandırma planlaması
- Omurga anahtarlar üzerinden TAP/SPAN konfigürasyonu ve Cyber Command kurulumu
- False positive oranlarının azaltılması, alarm analizi ve optimizasyonu desteği
- SOC analistleri için derin paket inceleme (DPI) ve platform adli bilişim eğitimleri

Çalışma Akışı

1. Trafik Toplama ve İzleme
- Tüm ağ segmentlerinden ayna trafik verisi alınır.
- Şifreli ve açık trafik akışları sürekli izlenir.
- Ağ bileşenlerinin iletişim haritası çıkarılır.
- Protokol ve paket analizleri merkezi sisteme iletilir.

→

2. AI Tabanlı Davranış Analizi
- Profil dışı sapan hareketler ve anomaliler aranır.
- Tehdit istihbaratı ile zararlı bağlantılar eşleştirilir.
- Saldırı adımları MITRE ATT&CK ile ilişkilendirilir.

→

3. Koordinasyon ve Müdahale
- Entegre Firewall üzerinden saldırgan IP'si engellenir.
- Entegre EDR ile enfekte uç nokta izole edilir.
- Detaylı adli analiz ve SOC raporları oluşturulur.

↗ **Sürekli İzleme**
Sangfor Athena NDR altyapısı, ağdaki trafik modellerini sürekli öğrenerek kendi makine öğrenimi modellerini optimize eder; yeni nesil tehdit varyantlarına karşı algılama doğruluğunu düzenli olarak artırır.

Avantajlar

Gelişmiş Şifreli Trafik Analizi (ETA)
Şifreli ağ trafiğini çözmeden (decryption yapmadan), paket boyutu ve zamanlama gibi meta verileri yapay zekâ ile analiz ederek gizli zararlı aktiviteleri yüksek doğrulukla tespit eder.

XDDR Tehdit Korelasyonu
Sangfor Athena EPP ve Güvenlik Duvarı çözümleriyle entegre olarak ağdaki anomali bilgisi ile uç noktadaki işlem loglarını birleştirir; otonom ve kusursuz bir müdahale ekosistemi sunur.

Görsel Saldırı Zinciri (Kill Chain)
Karmaşık ağ alarmlarını anlamlı bir hikayeye dönüştürür. Saldırganın ağa nereden girdiğini, hangi cihazlara sıçradığını ve amacını grafik arayüz ile net şekilde gösterir.

Proaktif Tehdit Avcılığı
Ağ geçmişine yönelik kapsamlı veri analitiği araçları sunarak, güvenlik analistlerinin sistemlerde gizlenen gelişmiş kalıcı tehditleri (APT) proaktif olarak aramasına olanak tanır.

aa teknoloji

AA Teknoloji, modern haber merkezleri için geliştirilen yapay zekâ destekli medya teknolojileri platformudur. Haber akış sistemlerinden dijital arşiv çözümlerine, gerçek zamanlı yayın altyapılarından çok kanallı içerik yönetimine kadar uzanan entegre çözümlerimiz; medya kuruluşlarının dijital dönüşüm süreçlerini hızlandırır ve ölçeklenebilir yayın operasyonları sunar.

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