aa teknoloji

Cortex XDR

Kritik altyapılar için tasarlanan Cortex XDR; uç nokta, ağ ve kimlik verilerini bütünleşik işleyerek siber tehditleri anında durduran ve operasyonel özgürlük sağlayan yeni nesil bir siber savunma platformudur.

Kurumsal Altyapı Güvenliği Zorlukları

Günümüzde siber saldırılar eskisinden üç kat daha hızlı gerçekleşmekte ve vakaların %20'sinde ilk sızma ile veri sızıntısı arasındaki süre bir saatin altına inmektedir. Geleneksel güvenlik araçları, proaktif koruma sağlamakta yetersiz kalarak altyapıları risklere açık bırakmaktadır.
Mevcut çözümler, bağlamdan yoksun ve düşük öncelikli çok sayıda alarm üreterek analistleri iş yükü altında ezmektedir. Bu durum siber operasyon merkezlerinde maliyetleri artırırken, operasyonel yükü de tırmandırmaktadır.
Farklı katmanlarda bağımsız çalışan izole araçların yarattığı görünürlük açıkları, sinsi tehditlerin ağda tespit edilmeden gizlenmesine yol açar.

⚠ Hang Ekiplere Hitap Eder?

- Aşırı alarm yoğunluğu altında siber yorgunluk çeken SOC ekipleri için
- Zero-day ve imzasız gelişmiş saldırıları engellemek isteyen yapılar için
- Farklı katmanlarda kör noktalar ve görünürlük açığı yaşayan kurumlar için
- Manuel analiz süreçleri yerine anında ve otomatik yanıt hedefleyenler için

Temel İlkeler

Önleme
Tehditleri sızmadan önce engeller.

Görünürlük
Tüm altyapıda tam görünürlük sunar.

Otomasyon
Analiz süreçlerini otomatikleştirir.

Verimlilik
Tek platformda maliyetleri düşürür.

Teknik Özellikler

Gelişmiş Tehdit Önleme
- Davranışsal analizle tehditleri engelleme
- Yapay zekâ destekli sıfır gün koruması
- Bilinen ve bilinmeyen zafiyet koruması
- USB ve Bluetooth cihaz kontrol yönetimi

Veri Analizi ve Algılama
- Tüm katmanlardan zengin veri toplama
- Yapay zekâ ile %98 alarm temizleme
- MITRE standartlarında tam uyumlu analiz
- Tehditleri kök nedenine kadar izleme

Olay Müdahale ve Yanıt
- Canlı terminal ile anında uzaktan erişim
- Otomatik müdahale ve karantina adımları
- Saldırı zincirini tek ekranda izleme
- Tehdit avcılığı için gelişmiş sorgular

Modüler Güvenlik Yönetimi
- Bulut çalışma zamanı ve konteyner güvenliği
- Kimlik tehdit algılama ve yanıt sistemi
- Yapay zekâ tabanlı gelişmiş e-posta koruması
- Veri sızıntısı önleme entegrasyonu

Sıkılaştırma ve Kontrol
- USB ve harici cihaz erişim yönetimi
- Yerel güvenlik duvarı ve disk şifreleme
- Mobil cihazlar için kurumsal koruma
- Ajan tabanlı yapay zekâ asistan desteği

Cortex XDR Nasıl Çalışır?

Cortex XDR; uç nokta, ağ, bulut ve kimlik verilerini kesintisiz toplayarak tek bir merkezde birleştirir. Gelişmiş yapay zekâ analizleriyle görünmeyen tehditleri tespit eden üç adımlı akıllı bir savunma döngüsü sunar.

Çalışma Akışı

1. Bütünleşik Görünürlük
- Tüm katmanlardan kesintisiz log toplar.
- Farklı verileri otomatik ilişkilendirir.
- Ağ genelinde kör noktaları yok eder.
- Analiz için temiz ve zengin bir veri sağlar.

→

2. Analiz ve Algılama
- Yapay zekâ ile davranışsal analiz yapar.
- Sıfır gün ve sinsi tehditleri anında saptar.
- Milyonlarca önemsiz alarmı otomatik eler.
- Kritik siber olayları öncelikli olarak sunar.

→

3. Soruşturma ve Yanıt
- Tehdidin kök nedenini tek ekranda gösterir.
- Canlı terminal ile uzaktan müdahale sağlar.
- Etkilenen sistemleri hızla karantinaya alır.
- Otomatik kurallarla tehdidi anında durdurur.

Esnek Entegrasyon ve Ölçeklenebilirlik
Cortex XDR, mevcut güvenlik yatırımlarınızla ve üçüncü parti mimarilerle tam uyumlu çalışır. Altyapınız büyüdükçe bulut tabanlı yapısıyla ek maliyet getirmeden sorunsuz ve esnek şekilde ölçeklenir.

Avantajlar

Yapay Zekâ Analitiği
Makine öğrenimiyle geleneksel araçların kaçırdığı karmaşık ve imzasız siber saldırıları proaktif olarak tespit eder.

Bütünleşik Veri Analizi
Uç nokta, ağ, bulut ve kimlik verilerini ilişkilendirerek altyapı genelindeki tüm kör noktaları ortadan kaldırır.

Akıllı Alarm Gruplama
Milyonlarca uyarıyı inceleyerek tek bir anlamlı olay zinciri haline getirir ve siber ekiplerin iş yükünü büyük oranda azaltır.

Canlı Müdahale Yeteneği
Live Terminal özelliği sayesinde uzak sistemlere anında erişim sunarak siber tehditlerin yayılmasını saniyeler içinde engeller.

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.